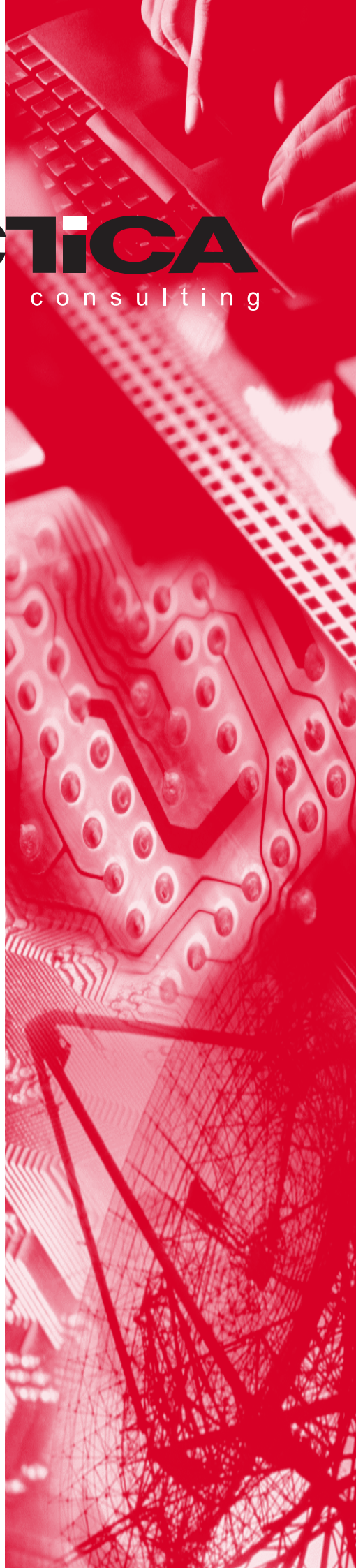

London Elections 2012 Independent Technical Assurance Report

ACTICA/PB333D014-1.0

List of Contents

INTENTIONALLY BLANK

Executive Summary

This document has been prepared by Actica Consulting Ltd (Actica) for the Greater London Authority (GLA). It contains the findings from the assurance activities undertaken during the preparation and conduct of the electronic count of the 2012 London elections.

Actica provided technical assurance from the early stages of the contract through to the count itself, conducted on 4 May 2012. This included the evaluation of design documentation and specifications, assessment of the system architecture and implementation, review of processes and procedures undertaken by the supplier, IntElect, witnessing and review of testing activities, conduct of security testing at key stages of development, assessment of the system build and deployment activities and an evaluation of system operation during the count.

The review identified that the system provided by IntElect had a sound technical and security architecture which included high capacity computing, networking and scanning equipment, a scalable and flexible software application, duplicate and spare components to provide resilience and controls to mitigate the principal security risks. Independent security testing confirmed that the technical controls were implemented appropriately, augmented by physical and procedural measures where necessary.

User Acceptance Testing was undertaken in two phases. The first phase verified the overall functionality of the core counting system and the second phase provided good confidence that the functionality and usability of the solution would be appropriate to undertake a successful count.

Comprehensive testing of the count lifecycle was performed and performance testing demonstrated that the system could operate at the level of the expected number of ballots for the live count. Resilience tests were undertaken to verify that the system could continue with the loss of single components and provided assurance that the system would have the required availability during the count, although the tests were not as comprehensive as had been recommended.

In summary, the electronic counting solution was designed, developed and deployed to a high standard, resulting in a successful count held on 4 May 2013. While there were some delays in completing the count, it is considered that the problems were not due to the capabilities of the system but rather due to external events and how the system was used.

The assurance activities conducted throughout the lifecycle of the system were valuable in highlighting issues at an early stage and helping to resolve them. This included aspects related to the functional specification, architecture, security implementation, testing, deployment and operational processes, and helped to ensure that the solution met the requirements. A number of significant issues were identified which, if not addressed, could have compromised the success of the count. Details of the major issues identified, and their effective resolution, are contained within this report. Some recommendations for enhancements to the detailed technical implementation and operation have been made for future elections.

INTENTIONALLY BLANK

1 Introduction

1.1 General

1.1.1 This document has been prepared by Actica Consulting Ltd (Actica) for the Greater London Authority (GLA). It contains the findings from the assurance activities undertaken during the preparation and conduct of the electronic count of the 2012 London elections.

1.2 Context

1.2.1 The GLA is London's strategic government. It includes an elected Mayor and 25 Assembly Members (14 Constituency Assembly Members and 11 London wide Assembly Members). Elections take place every four years and, as in previous years, the 2012 elections have involved manually marked ballot papers being counted electronically (e-counting).

1.2.2 The provision of e-counting services for the 2012 election was managed by London Elects and undertaken by IntElect, its supplier of e-counting services. Given the importance of the election working accurately, efficiently, effectively and securely on polling day, and the fact that the date of the election could not be moved, the GLA employed Actica to provide independent testing and assurance.

1.2.3 Actica provide technical assurance from the early stages of the contract through to the count itself, conducted on 4 May 2012. This included the evaluation of design documentation and specifications, assessment of the system architecture and implementation, review of processes and procedures undertaken by IntElect, witness and review of testing activities, conduct of security testing at key stages of development, assessment of the system build and deployment activities and an evaluation of system operation during the count.

1.3 Objective

1.3.1 The objective of this report is to provide an overview of the technical assurance activities undertaken to provide confidence in the system and the results arising from these activities.

1.4 Status

1.4.1 This version of this document is the full draft of the independent technical assurance report for final review.

1.5 Structure of this report

1.5.1 The remainder of this report is structured as follows:

a. Section 2 provides background information relating to the electronic count;

b. Section 3 describes the assurance activities, findings and subsequent actions relating to the design and specification of the electronic counting solution;

c. Section 4 describes the assurance activities, findings and subsequent actions relating to the development and initial testing of the electronic counting solution;

d. Section 5 describes the assurance activities, findings and subsequent actions relating to the final software testing and build of the electronic counting solution;

e. Section 6 describes the assurance activities, findings and subsequent actions relating to the operation of the count; and

f. Section 7 describes the conclusions of the assurance activities.

2 Background Information

2.1 Introduction

2.2 The plan for electronic counting

2.2.1 IntElect's programme of work to deliver the e-counting solution for the London elections in 2012 was based around the following stages:

a. Stage 1: Blueprint, covering the specification of the processes and systems to be used for the electronic count, originally scheduled for November 2010 to February 2011;

b. Stage 2: System development and testing, consisting of three phases:

   1. completion of application implementation, originally scheduled for February 2011 to September 2011;

   2. initial User Acceptance Testing, originally scheduled for September 2011 to December 2011; and

   3. final User Acceptance Testing, originally scheduled for December 2011 to February 2012;

c. Stage 3: Election preparation, originally scheduled for February 2012 to April 2012 and consisting of the following elements:

   1. completion of the training programme;

   2. printing and delivery of ballot papers; and

   3. final software testing and build of the system;

d. Stage 4: Election period, consisting of the following elements:

   1. the election week from 30 April 2012 to 3 May 2012;

   2. the election, to be held on 3 May 2012;

   3. the electronic count, to be held on 4 May 2012;

   4. data handover, from 7 May 2012 to 11 May 2012; and

   5. retention (by the GLA), from 14 May 2012 to 13 June 2012.

2.3 Assurance activities

Approach

2.3.1 The nature of the project, with a firm and fixed date for the election, meant that there could be no slippage in the schedule and timeliness of delivery was critical.

2.3.2 The assurance activities were undertaken through a mixture of document reviews, discussions with GLA and IntElect personnel, observation of the processes undertaken, analysis of technical information, review of the source system code and undertaking security testing of the implemented solution.

2.3.3 Assurance findings were fed back immediately, by email and verbally, and later summarised in a number of reports issued to GLA throughout the project lifecycle.

INTENTIONALLY BLANK

3 Stage 1: Design and Specification

3.1 Introduction

3.1.1 This section describes the assurance activities undertaken during the design and specification stage of the project.

3.2 Blueprint

Blueprint development and assurance activities

3.2.1 IntElect started work on the development of the electronic counting solution for the election in 2010. The first task was to develop the Blueprint that described the organisational structures, processes and the specifications for the technical components to be deployed in order to deliver the electronic count solution for the London 2012 elections.

3.2.2 The Blueprint consisted of 25 documents covering the project strategy and planning, functional and other specifications, technical overview and planning and procedural documents relating to the conduct of the electronic count. Early versions of some of the documents were received from the GLA in February 2011 and the baseline version of the Blueprint was released to Actica on 27 May 2011 for evaluation.

Findings from the Blueprint evaluation and subsequent actions undertaken

3.2.3 The specification contained in the Blueprint was assessed to be broadly appropriate for the delivery of a successful count.

3.2.4 The functional specification contained a sufficient level of detail about the counting functionality to be delivered and provided some confidence that an appropriately designed and implemented system would have the required capability to count the ballot papers. However, the technical information contained in the Blueprint was at a high level and there was little technical architecture and design information. A number of issues were identified:

a. The Business Continuity Plan was very general and related to general business activities rather than the London 2012 election. It was recommended that a specific London 2012 election Business Continuity Plan should be produced. This was subsequently developed and issued in March 2012.

b. The input data for the election system was to be collected via a web-based application that was less secure (by virtue of its access from anywhere connected to the internet) than the counting system itself. It was recommended that processes should be implemented to verify the correctness of the output data through comparison with offline material in order to detect any malicious activity to modify the data on the portal. Procedural checks were subsequently put in place to ensure that the material from the portal was verified by the Returning Officers.

c. The proposed solution to authenticate the officials operating the counting system involved the use of bar-coded badges. While this had been used at previous electronic counts in London and Scotland, it was assessed to be not sufficiently secure due to the ease in which credentials could be counterfeited. It was recommended that a more secure form of authentication was used. Following the Blueprint review, a more secure method of authentication was designed and developed using cryptographic smart cards.

d. The high-level architecture identified that a number of visual display components were to be located outside the restricted entry area of the count in order to provide progress information to observers. It was recommended that these visual display components should be separated from the counting network with a firewall in order to protect the counting system from attack from malicious personnel with access to these locations. It was further recommended that an intrusion detection monitoring capability should be introduced in order to detect any attacks or attempted attacks. These recommendations were put into place for the electronic count in May 2012.

3.2.5 There were also some gaps identified in the functional specification and technical overview, and these were highlighted to London Elects and the supplier so that they could be addressed. This included further information on the following topics:

a. Counting verification processes and how exceptions would be dealt with, such as processing the back of the ballot papers, dealing with marks that could identify the voter or blank ballot paper processing. Many of these related to areas where the requirements from London Elects had not been decided. These were subsequently finalised and taken into account during the design and implementation phase.

b. How the back-up and restoration of data would be undertaken to provide assurance regarding the integrity of the backed up data. These processes were not subsequently developed although they were highlighted at a number of points during the lifecycle.

c. How data stored on the scanners would be erased. A process for deleting data on the scanners, which used the same approach as for the other components, was subsequently provided.

d. How the resilience and robustness of the solution, and in particular the central servers, would be ensured. Following the review feedback, a document was prepared which outlined the approach resilience, including the use of redundant and spare components at all levels of the system. This was assessed as part of the technical architecture review carried out in the next phase.

e. How the VPN and firewalls would be configured, to ensure the security of the solution. The high-level configuration was provided following the Blueprint review and the detailed configuration provided during the testing phase.

f. A description of the architecture diagrams to ensure that the high-level technical architecture could be effectively assessed. This was provided and assessed as part of the technical architecture review.

3.2.6 Some modifications to the proposed processes were also recommended:

a. Some enhancements to GLA's test strategy were required to ensure that sufficient confidence could be obtained from the testing process. These were incorporated into the user acceptance testing processes.

b. The strategy and approach for development and integration testing was not included in the Blueprint and it was recommended that this information should be included within the assurance process. Detailed testing plans were subsequently provided.

c. There were some inconsistencies and ambiguities in the functional specification and it was recommended that this was addressed. An updated version of the Blueprint was released in November 2011 which resolved the significant issues.

d. The documentation provided was not marked and it was recommended that security classifications were applied to sensitive documents to ensure correct handling. The

Government Protective Marking System was applied to subsequent sensitive documentation.

3.3 September 2011 progress report

3.3.1 An assurance progress report was produced in September 2011 which reported on the end of the Design and Specification stage. At the time the report was written, revised documentation had not yet been issued to address the issues identified in the original Blueprint review. Some design information had been presented, but no comprehensive design or implementation information had been provided. The review therefore concluded that the level of detail in the documents made available for assurance to date had not been sufficient to give a high degree of confidence in the solution. More detailed technical information was subsequently provided following this progress report.

3.3.2 The review acknowledged, however, that while there was a delay in the undertaking of the Blueprint review process and delays in the provision of design and implementation information, the GLA had started planning and preparation of the Election earlier than in previous years and there was some contingency in the project schedule to accommodate the delay that had occurred.

INTENTIONALLY BLANK

4 Stage 2: Development and Initial Testing

4.1 Introduction

4.1.1 This section describes the assurance activities undertaken during the development and initial testing stage of the project.

4.2 Architecture development

Architecture design and assurance activities

4.2.1 IntElect developed the system design and architecture extending the very high-level view described in the Blueprint. The software was developed using the Scrum agile software development methodology. A number of technical architecture diagrams and technical configuration documents were provided by IntElect, although no formal system design document was produced. The technical architecture evaluation was undertaken through a review of this documentation, validation against the source code base, holding discussions with IntElect staff and through direct observation of the system.

Findings from the architecture evaluation and subsequent actions undertaken

4.2.2 The review identified that the IntElect system had a sound technical architecture. Aspects covered by the review included the following:

a. Hardware: The solution included a sufficient number of high-throughput scanners to process all envisaged ballot papers within the allotted window. The system was to be hosted on appropriate enterprise-level servers, networking equipment and desktop access devices. There was planned to be ample storage and computing capacity to handle the expected workload with the required level of performance.

b. Software: The software application was designed using a service-oriented architecture developed using standard best-practice architectural components and frameworks. The architecture was modular, loosely-coupled and standards-based, which ensured that it could be easily modified, updated and extended. It was scalable and flexible, with the ability to re-assign resources and increase overall capacity by adding additional hardware and software components.

c. Resilience: Resilience and redundancy issues had been considered by the supplier and there were duplicate and spare components for all aspects of the system, including both online host standby and offline cold standby components.

d. Security: At a high level, the technical security architecture was sound. The solution was designed as a closed system, with no external interfaces during the count. Communications between sites was to be achieved across the internet, protected using an encrypted tunnel, firewalls and further application-layer encryption. Physical security controls were intended to protect the equipment before and during the count. User access was to be controlled by two-factor authentication (smart card and PIN).

4.2.3 A number of architectural security issues were, however, identified. The issues found during the Blueprint review, relating to the need to separate the display functionality and to validate web portal data, had not been addressed and were re-iterated. In addition, there were a number of issues that could potentially be exploited in conjunction with other attacks:

a. There was a risk that an insider with access to the code base could install malicious software or corrupt existing software to compromise the integrity of the election. It was recommended that all software modules should be digitally signed and only allowed to execute if they had an appropriate signature. This was coupled with the recommendation for extensive testing to ensure the signature process did not compromise the availability of the system. When this was subsequently considered by IntElect, it was assessed that there was insufficient time to undertake the change and the necessary testing before the election. Instead, cryptographic hashes were taken for all modules during system build and a manual compare was undertaken immediately prior to live operation at the count centres. This provided assurance that compromise of the application in the period between system build and live operation would be detected, although it did not fully protect against all attacks to the software application. It is recommended that full digital signatures are implemented for future elections.

b. There was a lack of mutual authentication for information exchanges between components within the system. While this vulnerability would not be exploitable on its own, it would enable an attacker that gained access by another vulnerability to cause more damage. Mutual authentication was subsequently implemented on the system to address this.

c. The proposed web portal system had a password reset process that was not sufficiently secure and was vulnerable to masquerade and eavesdropping attacks. It was recommended that a more secure process was implemented involving secure communications with known administrative contact points. This was subsequently implemented.

4.3 Initial User Acceptance Testing

Initial User Acceptance Testing and assurance activities

4.3.1 The first period of User Acceptance Testing (UAT1) was undertaken between 21 and 23 November 2011 in accordance with the project plan. The aim was to demonstrate and verify the functionality of the core counting system, from batch registration through to result declaration.

4.3.2 The UAT1 configuration consisted of a two-host server and a single count site comprising three constituencies. Each constituency was approximately one third of the size of a full constituency. A full count was undertaken, testing registration, scanning, verification, adjudication and declaration functionality using ballot papers prepared by London Elects. The site was connected to a simulated central site hosted on the same server platform. Simulated activities from the other two constituencies were conducted in parallel to provide a further load on the servers.

Findings from the initial User Acceptance Testing

4.3.3 Observation of UAT1 activities indicated a well-planned event that provided a thorough test of the core parts of the applications, although neither a formal test specification for UAT1, nor a report describing the outcome, was provided. The scanners were operated by London Elects and council employees and there was a high-degree of input into the user acceptance testing process from London Elects, including the scope and format of the testing. This enabled a representative assessment of the functionality and usability of the system to be obtained.

4.3.4 The outcome of the UAT1 activities was measured by London Elects against the previously-defined success criteria, which were broadly demonstrated to have been have been achieved, although a small number of components were deferred until later stages. Items not demonstrated during UAT1 included web portal functionality, data import, user registration, visual display output and backup processes.

4.3.5 The UAT1 system server logs were supplied and analysis revealed that the process, disk and network usage figures were all well within the available capacity, with sufficient headroom when scaling for live operation was taken into account. Memory utilisation figures were also within capacity, but closer to the maximum available. It was recommended that memory usage should be further monitored during the performance and resilience tests.

4.3.6 Comprehensive security testing was undertaken on the UAT1 configuration, covering the hardware assurance, software assurance, code review, network and communications assurance and database assurance activities. The results are described in the Section 4.4 of this report.

4.3.7 The overall approach to UAT1 demonstrated good involvement and communication between the organisations and provided confidence that the system would meet the business requirements. Observation and technical discussions held during the first period of UAT provided confidence that the system was on track to be fit for purpose for the election.

4.4 Implementation

Implementation and assurance activities

4.4.1 An assessment was undertaken of the development approach and a code review was undertaken involving source code analysis of the code base. Comprehensive security testing was undertaken on the configuration used for user acceptance testing. The testing assessed the vulnerabilities associated with the hardware, operating system, database and application software, network, firewall and telecommunications infrastructures.

Findings from the implementation evaluation and subsequent actions undertaken

4.4.2 An agile system development methodology was used with a time-boxed approach to internal software releases. These were produced on a bi-weekly basis and were subject to functional testing, which was well-resourced with four full-time testers allocated to the project. Peer review processes took place in a number of areas, although a full formal record was not created, partially due to time pressures. While we were not given access to a full set of information to verify the exact processes undertaken, the development and unit testing processes appeared to be well addressed and followed good industry practice. The code review confirmed the maturity of the development processes and demonstrated a commitment to produce high-quality, secure code.

4.4.3 It was not possible to compromise the result of the election, even with direct access to the system, and there was evidence that some security hardening had been undertaken with many unnecessary programs removed from the system and a number of security checks enabled on the firewalls. It was not possible to bypass the smart card secure authentication.

4.4.4 However, a number of significant vulnerabilities were identified with the configuration, a number of which could have led to a compromise of the election result if exploited by an attacker with sufficient system knowledge, time, resources and expertise. In some cases the identified vulnerabilities applied to individual machines only and there were further machines that did not demonstrate the vulnerabilities, suggesting a configuration error rather than a fundamental issue. In other cases, the vulnerabilities reflected issues that would need to be resolved prior to deployment. The main vulnerabilities with the system arising from the security testing were summarised as follows:

a. The configuration of the scanners, PCs, switches and firewalls needed to be further hardened by disabling non-required functionality and services that could be used to compromise the system. These issues were addressed prior to the count.

b. The firewall rules needed to be strengthened to restrict traffic to the minimum necessary and the VPN encryption configured needed to be strengthened to reduce the risk of a successful attack. These issues were addressed prior to the count.

c. There were insufficient network segregation controls to separate the communications and display functionality from the e-counting system. The architecture was changed and firewall separation implemented prior to the count.

d. Account and password implementation needed to be strengthened, including system policies, use of network accounts, database account management and authentication processes. These issues were addressed prior to the count.

e. There were a number of programmes installed, including command shells and management services, that were unnecessary and could be used by an attacker to compromise the system. These programmes were removed prior to the count.

f. Anti-virus software was not installed on a number of machines, such as the desktop PCs. Following the issue of the testing report, anti-virus software was installed on all components. A full scan of the system was taken following installation at the count centres, immediately prior to the count. The anti-virus software was then disabled to reduce the performance impact on the count. This represented a compromise between the risks to the security and performance of the system.

g. A number of monitoring and logging services were not enabled and, in some cases, the security log was too small to hold the required information. These issues were addressed prior to the count.

h. Some of the third-party software installed was outdated and needed to be upgraded to the latest version. Not all important security patches had been applied. The majority of these issues were addressed prior to the count. There remained a small number of minor configuration vulnerabilities that could not be resolved without increasing significantly the preparation for the count; it was assessed that the vulnerabilities presented a low risk to the count.

i. There were a number of instances where access rights for users, files and directories had not been correctly set. The majority of these were addressed prior to the count, although it was not possible to address all of them as the effect on the success of the system could not be assured within the timescales.

j. There were a number of interfaces, such as USB sockets, that were not physically protected. The systems were subsequently hardened to restrict the ability of an attacker to exploit the physical interfaces and it was planned that the systems would be located within an access-controlled area under observation. However, it was noted that observers would not be able to differentiate between authorised and non-authorised system maintenance and it was recommended that regular inspections should be undertaken of

the installed system by IntElect maintenance personnel before, during and after the count to ensure that any tampering would be detected. Inspections were undertaken at the count site before and after the count, although the inspections were not conducted as regularly as had been recommended.

4.4.5 It was recommended that further security testing should be undertaken following the second period of User Acceptance Testing (UAT2) to verify that the vulnerabilities had been adequately addressed. This was subsequently undertaken.

4.4.6 The visual display system had not been finalised at the time that the security tests were undertaken and it was further recommended that security testing should be subsequently undertaken on the visual display units that were not included within the current scope. This was subsequently undertaken.

4.5 December 2011 progress report

4.5.1 An assurance progress report was issued in December 2011. It concluded that the technical architecture was sound and that no substantial re-design was required in order to undertake a successful election. The hardware specified had sufficient performance to undertake the count within the required timescales and the system architecture included multiple features to provide resilience.

4.5.2 The main issues identified were that there had been some delays in the development and testing processes. Insufficient testing information had been made available, particularly regarding performance and resilience testing, to provide full assurance for the system implementation. A number of security vulnerabilities had been identified in the UAT1 configuration that would need to be addressed before UAT2.

4.5.3 It was also noted that a review of security and service management procedures would be necessary to ensure suitability of the overall service at the time of the count.

4.6 Second period of User Acceptance Testing

Second period of User Acceptance Testing and assurance activities

4.6.1 The second period of User Acceptance Testing (UAT2) was undertaken for functional aspects in February and March 2012. A separate process was adopted for UAT2 for non-functional aspects.

4.6.2 A functional UAT2 test was undertaken on 2 February 2012 and involved the operation of a count of approximately 25,000 ballot papers.

Findings from UAT2 and subsequent actions undertaken

4.6.3 Testing focussed on the issues identified in UAT1 and their resolution, although no formal specification for UAT2 was provided. The tests included modifications to the scanning thresholds and ballot paper zones to reduce the number of papers that are flagged up for adjudication due to folds or minor damage to the edges. The functional testing was assessed to be appropriate.

4.6.4 Following UAT2, a small number of outstanding issues continued to be tracked using a Joint Issues Log. The impact of the outstanding issues on the overall success of the count, provided the identified remediation was applied, was expected to be minor.

4.6.5 The UAT2 activities provided good confidence that the functionality and usability of the solution would be appropriate to undertake a successful count.

4.6.6 Initial performance testing indicated that the hardware was likely to have sufficient capacity to fulfil the count, although full performance testing was planned for later in the project. While there was some anecdotal evidence of load balancing and resilience testing, it was not comprehensive. It was recommended that comprehensive resilience testing should be undertaken, covering failure of all major components, including third party software components. It was also recommended that full stress testing was undertaken during the performance testing phase to test the resilience of the server processes.

4.7 March 2012 progress report

4.7.1 An assurance progress report was issued in March 2012, which reported on the end of the Development and Initial Testing stage. It concluded that the overall architecture and implementation of the system was sound and sufficient to deliver a successful count.

4.7.2 The majority of the security vulnerabilities that were detected in the UAT1 configuration had been addressed in the UAT2 configuration. However, the report noted a number of issues for resolution:

a. Insufficient testing results had been made available regarding performance and resilience testing to provide assurance in the system implementation. This was noted as an increasing risk.

b. There remained a number of security vulnerabilities in the UAT2 configuration that needed to be addressed before system lock-down. These included import data validation, network segregation and code signature issues.

c. Formal release, change and configuration management processes were required for the reference system to be deployed at the count sites.

d. A number of operational processes needed to be defined and documented covering security management and service delivery.

4.7.3 These issues were subsequently addressed and are discussed in Section 5.

5 Stage 3: Final Software Testing and Build

5.1 Introduction

5.1.1 This section describes the assurance activities undertaken during the final software testing and build stage of the project.

5.2 Final testing

Final software testing and assurance activities

5.2.1 Final software testing was undertaken prior to finalising the development activities. IntElect had a mature process for testing, assisted by a comprehensive performance testing plan and a test environment involving 'robots' that could simulate manual operation of the system. This enabled effective performance testing of the system.

5.2.2 The testing assurance processes consisted of a review of the test plans, observation of a subset of the testing and analysis of the results.

Findings from the final software testing and assurance activities and subsequent actions

5.2.3 The final test plans were reviewed and comments provided to ensure the comprehensiveness of the testing, particularly relating to end-to-end, stress and resilience testing aspects.

5.2.4 Comprehensive testing of the count lifecycle (from registration to result declaration) was performed, but there was little evidence at this stage of resilience testing or full system end-to-end testing, covering communications with the central site, public visual display outputs and back-up activities. There was subsequently some coverage of these aspects at the build stage, described in Section 5.3.

5.2.5 Due to the nature of the project, in which the go-live date cannot be moved, and due to some delays in previous stages of the project, there was insufficient time to undertake the range of testing specified in the performance test plan. Nevertheless, the testing covered all aspects of the count (registration through to adjudication) at some level across a number of system configurations and demonstrated that the system could operate at the level of the expected number of ballots for the live count.

5.2.6 A number of database errors were observed during the scanning and adjudication performance tests, including deadlock errors and the inability to close or lock batches. These were likely to have arisen from minor bugs in the application code that manifested when the system was operating in high degrees of concurrency. The application had been coded to retry the relevant action in these situations and the net result was a reduction in performance rather than the failure of the application. Following the testing, the application software was updated to address these issues.

5.3 Build testing

Build testing and assurance activities

5.3.1 IntElect had an Acceptance Test Plan that aimed to demonstrate the e-counting system built for the London 2012 elections was configured in accordance with the approved solution design, was fit for purpose and was sufficiently reliable to support the expected production volumes. It covered performance, resilience, security and functionality, including import/export and configuration (access rights) aspects, and represented a reasonably comprehensive set of tests to provide confidence in the as-built system.

5.3.2 The build testing assurance processes consisted of a review of the test plan, observation of a subset of the testing and analysis of the results.

Findings from the build testing and assurance activities and subsequent actions undertaken

5.3.3 The build test plans were reviewed and comments provided to ensure the comprehensiveness of the testing, particularly relating to stress and resilience testing aspects.

5.3.4 The configuration test plans included verification that the range of user roles were able to log on and access the required functionality. They also included a number of end-to-end tests to verify communications with the central site, the visual display output, the external web site and the provision of back-ups.

5.3.5 The acceptance test process included provision to add new build tests when further issues were identified concurrently.

5.3.6 The performance tests involved a representative load (with some headroom) of 3,500,000 ballots in total for a five constituency count site. These were successfully executed within the required timing parameters, providing further assurance in the ability of the software to deliver a successful count. It was reported that the database errors previously encountered during performance testing had been fixed.

5.3.7 The resilience tests involved verification that the system could continue with the loss of single components, including a single server (physical platform and virtual server), network switch (both core and edge), scanner, operator terminal, database instance, load balancer, disk drive and the internet connection (which supported the connection to the central site). These tests proved successful.

5.3.8 The resilience tests did not, however, cover the loss of other central components such as the distributed transaction or message queue servers, service bus, disk controller, network controller or communications server. While these components are inherently more resilient than the single components that were tested and so failure was not likely, the impact of failure on the count, should it occur, was likely to be large.

5.3.9 The security tests involved a number of tests to check that access was denied when actions were attempted that should not be permitted, and that the required security hardening controls were in place. They provided a good level of due diligence to complement the penetration testing assurance activities, although there were a small number of aspects that were omitted from the testing schedule.

5.3.10 The set of acceptance test results received demonstrated that the Acceptance Test Plan had been partially executed. These showed that performance testing had been successfully carried out on

two of the count sites and that the majority of the configuration and security tests had been successfully completed. The resilience tests had only been partly completed and the end-to-end testing, including back-up testing, had not been conducted.

5.4 April 2012 progress report

5.4.1 An assurance progress report was issued in April 2012, which reported on the end of the Build and Release Testing stage. It concluded that there was good assurance that the e-counting system was fit for purpose, through a sound architecture and implementation and successful load testing. The main risk related to how the system would perform in unforeseen circumstances as the stress and resilience testing had been less comprehensive than planned.

5.4.2 Only medium assurance could be provided relating to the public visual display system. The architecture had been modified in response to the previously identified issues and was sound, but successful end-to-end testing had not taken place at the time of writing the progress report. Successful end-to-end testing was, however, achieved prior to the operation of the count.

5.4.3 The security of the built configuration was good and the majority of issues identified during testing had been fixed. Some known vulnerabilities remained, although these were minor and would be addressed through procedural means. The security of the wide area network remained a risk as it had not yet been implemented or tested; this was subsequently undertaken prior to the count. Controls against insider attack had only been partially implemented and there remained therefore a high degree of trust in the individuals responsible for configuring the system.

5.4.4 It was identified that insufficient information had been provided on the service delivery procedures and it was stated that these would be provided during the week leading up to the count.

INTENTIONALLY BLANK

6 Stage 4: Count Operations

6.1 Introduction

6.1.1 This section describes the assurance activities undertaken during the count operations stage of the project, covering system deployment, operations and decommissioning.

6.2 Deployment

Set-up and assurance activities

6.2.1 The electronic counting system was implemented over four geographic sites: three counting venues and a single central site. The three count venues were as follows:

a. Excel, which provided the counting capability for five constituencies: Bexley and Bromley, City and East, Greenwich and Lewisham, Havering and Redbridge, and Lambeth and Southwark;

b. Olympia, which provided the counting capability for five constituencies: Croydon and Sutton, Ealing and Hillingdon, Merton and Wandsworth, South West and West Central; and

c. Alexandra Palace, which provided the counting capability for four constituencies: Barnet and Camden, Brent and Harrow, Enfield and Haringey and North East.

6.2.2 The central site was implemented within the GLA City Hall. It supported progress and voting monitoring across all fourteen constituency counts as well as the London-wide voting calculations.

6.2.3 IntElect obtained access to the three count venues on the morning of 2 May 2012 and set up the equipment over the course of the 2 and 3 May 2012.

6.2.4 The following activities were undertaken on 3 May 2012:

a. observation of the IntElect processes during set up;

b. conduct of security tests; and

c. inspection of the e-counting equipment and its configuration.

Findings from the set-up assurance activities and subsequent actions undertaken

6.2.5 The e-counting equipment was set up successfully on the two days prior to the count. It is noted that implementing a system of moderate complexity, such as this electronic counting solution across four venues, over two days, represents a challenge.

6.2.6 IntElect followed a Technical Build document, which described in detail the activities required to install and configure the system. Some configuration problems were experienced by IntElect during the set-up process, where the configuration was not as expected from the build process. However, no serious issues were detected and the issues were resolved in time for kit readiness testing.

6.2.7 A hash function was performed on all executable files and the results compared with known results from the build process. This was undertaken to provide assurance that the system had not

been tampered with since the build stage. The process was observed at the Olympia count centre and indicated that all executable files had been installed as expected.

6.2.8 The kit readiness was observed at Olympia and Excel. This was conducted as per the Kit Readiness Guide in the Count Centre Manual and provided a methodical approach of checking that all components were functional as expected. The scope included issuing 20-30 smart cards to conduct the tests, preparing the system for the count, registering 30 batches of 100 ballot papers ensuring that each of the workstations was tested, scanning the ballot papers ensuring that each of the scanners was tested, verifying the batches, adjudicating the ballot papers as necessary, monitoring the progress of the count, closing the count and computing the results.

6.2.9 Engineering checks were made for the scanning equipment and logged in the Count Centre Manual as expected. A number of scanners required calibration or other engineering maintenance; however, no fundamental issues were identified with the technical systems at these two venues.

6.2.10 It was not possible to conduct a full range of security tests on the system as the testing activities had not been fully pre-arranged and IntElect were not able to allow direct access so close to the count. Assurance for the security of the implementation was therefore based on the security tests performed on the build system and IntElect's change and configuration management processes.

6.2.11 The tests that were able to be performed indicated that the system was appropriately set up and configured as expected, in accordance with the build system:

a. It was not possible to communicate with the system by plugging into spare ports on the networking equipment.

b. A vulnerability that had been identified during the build testing, which enabled an attacker to break out of the e-counting application to gain access to the underlying system, had been fixed.

c. The firewall rules at the central site were appropriate for the secure communication with the counting sites and the connection to public visual displays and GLA web site.

d. It was not possible to boot up the scanners from removable media plugged in to the back panel.

6.2.12 The following security issues were identified and alerted to GLA prior to the count:

a. It was possible to log on to the scanner basic input-output system (BIOS) using a password that was contained within the build documentation. The distribution of this document was limited to trusted personnel within IntElect, GLA and Actica, and it was assessed that the risk arising from this vulnerability was low, given the extent of the documentation distribution and the venue physical security. However, it represents poor password management practice in this instance.

b. There was some damage to the rear door of one of the server cabinets such that it would not close or lock. It is understood that increased guarding/vigilance was put into place to monitor this.

c. The power to the workstations, scanners and edge (constituency) switches was accessible to observers and in some cases there were insufficient barriers to keep them away, resulting in a few situations where there was a high risk of an observer cutting the power either maliciously or by treading on a power switch. IntElect were advised to ensure physical protection for the switches (where termination of power could cause a

constituency-level outage of a few minutes). Individual workstations and scanners were still at risk, but the impact on the count of isolated occurrences would be low.

d. Some of the edge (constituency) switches were positioned in their secure containers such that an observer would be able to tamper with the connections. While there were technical controls to ensure that the damage would be limited, an attacker could cause a loss of availability through unplugging equipment. IntElect was advised to turn round the containers such that the switches were only accessible from the inner area. This was addressed in one of the count centres.

6.3 Count

Count and assurance activities

6.3.1 The e-counting system had been successfully set up and was operationally ready for the morning of the count on 4 May 2012. The system administration function was largely support-oriented and consisted of the following main activities:

a. monitoring to verify that the system was performing appropriately;

b. resolving incidents as they occurred;

c. developing and installing system updates if incidents could not be effectively resolved within the constraints of the implemented system; and

d. creating backups at the end of the day and delivering them to the Greater London Returning Officer (GLRO) and Constituency Returning Officers.

6.3.2 The assurance activities for the count were undertaken through observation of the operation of the system and discussions with GLA and IntElect staff.

Findings from the count assurance activities and subsequent actions undertaken

6.3.3 The electronic counting activities were successfully completed during 4 March 2012. At two of the count centres, Excel and Olympia, the counting was concluded and the results produced well within the ten-hour counting window allocated.

6.3.4 There were, however, delays in the overall declaration due to issues at the Alexandra Palace count site. The power was turned off at Alexandra Palace at approximately 7.45am, reportedly for a sprinkler test. This was undertaken by venue contractor staff and was not within IntElect's control. A period of time was required for the system to shut down gracefully in accordance with the designed behaviour and, following resumption of power, to restore the system to the required level. When successful operation had been verified, the remaining systems were brought up and by 10.45am, three of the four constituencies were operational.

6.3.5 The time to recover each constituency was dependent on the state when the power went down. Some had already undertaken batch initialisation and zero count and could start the ballot box registration and counting activities relatively quickly. Brent and Harrow had not undertaken the zero count and additional time was required to recover as additional checks were needed to ensure that the system had been initialised properly; the overall delay for Brent and Harrow was over three hours.

6.3.6 There were further delays in the Brent and Harrow constituency as a number of postal ballot papers had been damaged prior to the count during the opening process within the local authority. The affected papers had been subsequently repaired but a large proportion of them

(approximately half) were not able to be scanned; this is several orders of magnitude higher than would be expected in a normal batch. Two batches that would not scan correctly were erroneously placed in the stack of scanned batches during the count which meant that the problem was not identified until later in the day. The substantial volume of manual entry resulted in further delays, on top of the previous days due to the power outage.

6.3.7 It is considered that the problems observed at the Brent and Harrow constituency count, which delayed the completion of the count, were not due to the capabilities of the system and would have resulted in further delays had it not been for the flexibility of the system which could be re-configured to enable papers to be manually entered in parallel. It is, however, possible that enhanced workflow monitoring could have identified the large numbers of ballots papers requiring manual entry at an earlier stage.

6.3.8 Although comprehensive procedures had been developed for the technical build of the system and the use of the application, there were no documented procedures for the system administration activities during the count. This meant that when unforeseen events occurred, such as the power outage at Alexandra Palace, recovery was reliant on the skills and expertise of a small number of personnel and there was a higher than necessary risk of extended delays. Despite the lack of documentation to bring the system back up, it is not assessed that the manual procedures resulted in significant delays to the recovery in this instance.

6.3.9 IntElect staff undertook a significant degree of monitoring of the solution, including application and infrastructure monitoring, to ensure that they were able to respond to the majority of incidents occurring in a timely and effective manner, although the level of monitoring undertaken across the count centres was not always consistent.

6.3.10 Some updates were required to the system during the count to facilitate its completion within the allotted time window. There was a process to approve and implement updates and patches, although it could not be verified whether this was followed.

6.3.11 The backup process had not been fully tested prior to the count and did not complete successfully. A workaround was developed on the night which involved manually copying the required files. There was no process for verifying the content of the backups and there was a risk that important information was not included in the constituency backups.

6.3.12 There was effective segregation of roles among system administrators and no single individual had full access to all aspects of the system. Good security discipline was observed regarding the use of screen locks.

6.4 Post-count

Post-count activities and assurance activities

6.4.1 Following the count assurance was undertaken for the following key processes:

a. post-count evaluation of the patching during the live count;

b. system closedown, backup and verification; and

c. data deletion and system disposal and re-deployment.

Findings from the post-count activities and recommendations

6.4.2 The patches deployed during live operation corresponded to those reported during the count and identified in the count report. The patches deployed were required to achieve smooth operation of the count.

6.4.3 Backups were taken of all count site and central systems. IntElect undertook some analysis of the central backups but no explicit backup verification was undertaken of the count centre backups. Full assurance cannot therefore be provided, although the risk is not considered high due to the technical and system knowledge and skills of the individuals undertaking the backups. Only the backup provided to the GLRO was encrypted and the protection of the information on the memory sticks provided to the Constituency Returning Officers will rely on the on-going physical protection of the media.

6.4.4 The full change process was only followed for the modification of the backup encryption functionality and was not followed for the remaining patches.

6.4.5 The approach taken to deleting the data on the servers and scanners did not ensure that all data was destroyed and it is likely that some trace of the data remained on these systems.

6.4.6 The approach taken to deleting the data on the laptop provides more assurance that the data had been destroyed. While the software used had not been independently evaluated, the tool contained the expected functionality required and the risk is considered very low that any significant data remained on the laptops.

6.4.7 It was recommended that for future election count events:

a. the change request process and authorisation process is fully documented prior to the count and followed for all system changes;

b. a backup verification process is developed prior to the count and conducted after the backups have been produced to ensure they contain the expected data;

c. all backups are encrypted to an appropriate level in accordance with Government Security Policy; and

d. data is deleted from all systems using appropriately assured data erasure software.

INTENTIONALLY BLANK

7 Conclusions

7.1 Introduction

7.1.1 This section describes the conclusions of the assurance activities.

7.2 Conclusions

7.2.1 The electronic counting solution was designed, developed and deployed to a high standard, resulting in a successful count held on 4 May 2012. While there were some delays in completing the count, it is considered that the problems were not due to the capabilities of the system but rather due to external events and how the system was used.

7.2.2 The assurance activities conducted throughout the lifecycle of the system were valuable in highlighting issues at an early stage to enable them to be addressed before the election. This included aspects related to the functional specification, architecture, security implementation, testing, deployment and operational processes, and helped to ensure that the solution met the requirements. Some recommendations for enhancements to the detailed technical implementation and operation have been made for future elections.