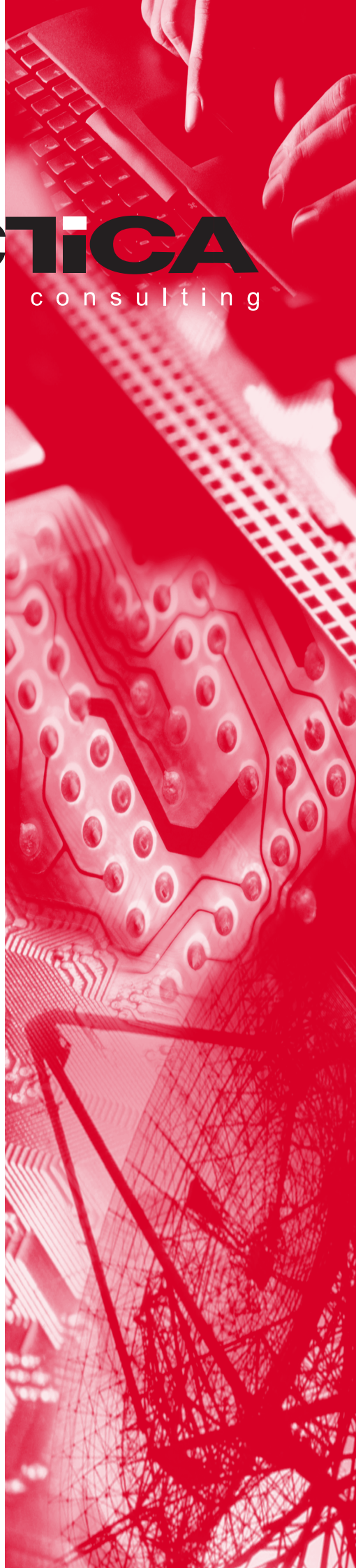

ACTICA consulting

Technical Evaluation of Rushmoor Borough Council e-voting Pilot 2007

ACTICA/PA468D009-1.1

31 July 2007

List of Contents

INTENTIONALLY BLANK

1 Foreword

1.1 Under the Representation of the People Act (RPA) 2000, any local authority in England can submit proposals to the Secretary of State for Justice (prior to 9 May, the Secretary of State for Constitutional Affairs) to carry out an electoral pilot scheme. Electoral pilot schemes can involve changes to when, where and how voting at local elections is to take place and how the votes cast at the elections are to be counted. The Electoral Commission has a statutory duty to evaluate and report on any pilot scheme approved by the Secretary of State.

1.2 A total of 312 local authorities in England held elections on 3 May 2007. In October 2006, the Department for Constitutional Affairs (DCA) and the Electoral Commission issued a joint prospectus to local authorities inviting applications for electoral pilot schemes at the May 2007 elections. Fourteen applications were received in response to the prospectus, from a total of 17 local authorities; one application was subsequently withdrawn. In January 2007 the Secretary of State for Constitutional Affairs announced that he had approved 12 of the pilot schemes in a total of 13 local authority areas. A full list of all the authorities which held pilot schemes in May 2007 is available on the Electoral Commission's website at www.electoralcommission.org.uk.

1.3 This report presents Actica Consulting Ltd's (Actica's) technical evaluation findings in support of the Electoral Commission's evaluation of the electoral pilot scheme in the borough of Rushmoor at the elections on 3 May 2007. It provides details of a technical evaluation of various aspects of the scheme, including: the management approach, the technical solution, the security provided, and the value for money.

1.4 The output of this report will be used by the Electoral Commission in support of their overarching scheme evaluation, which includes a description of the scheme and an assessment as to:

a. the scheme's success or otherwise in facilitating voting or the counting of votes, or in encouraging voting or enabling voters to make informed choices at the elections;

b. whether the turnout of voters was higher than it would have been if the scheme had not applied;

c. whether voters found the procedures provided by the scheme easy to use;

d. whether the procedures provided for by the scheme led to an increase in impersonation or other electoral offences, or in any other malpractice in connection with elections;

e. whether those procedures led to any increase in expenditure, or to any savings, by the local authority.

1.5 In addition to these statutory requirements, the Commission's evaluation also considers, where appropriate:

a. the extent to which the pilot scheme facilitated or otherwise encouraged participation among particular communities, including young people, ethnic minority groups and people with disabilities;

b. overall levels of user awareness and comprehension of the voting method being tested, including an assessment of the effectiveness of any literature or other materials used in the promotion of the pilot scheme;

c. the attitudes and opinions of key stakeholders, including voters, with a view to determining overall levels of confidence in the voting method being tested;

d. whether the pilot scheme resulted in measurable improvements, or had any adverse impact, with respect to the provision of more efficient and effective service delivery to voters;

e. whether the pilot scheme resulted in measurable improvements to, or had any adverse impact on, the existing system of electoral administration;

f. whether the pilot scheme represented good 'value for money';

g. where appropriate, the Commission may also make recommendations as to whether changes should be made to electoral arrangements more generally through roll-out of the pilot scheme procedures.

1.6 In preparing this technical evaluation report, Actica has drawn on its own observation and assessment of the pilot scheme, as well as on the views expressed to us by a number of other stakeholders. We would particularly like to thank the Returning Officer, the Electoral Services department of Rushmoor and the supplier of the electronic voting service, Election Systems and Software Europe Ltd (ES&S), for their assistance in undertaking this evaluation and for supplying us with the information and data to support it.

2 Introduction

2.1 Rushmoor Borough Council (the Council) has a strong track record of conducting pilot schemes at local elections, including:

a. An internet voting pilot, carried out in 2003, which required pre-registration. The time period available for internet voting was from 6.00am the Friday before the poll until the close of poll.

b. An advance voting pilot, carried out in 2006, which used a networked electronic register and 'ballot on demand' software that allowed electors to vote at advance polling stations in Rushmoor's two main town centres, or at a local military garrison.

2.2 Following the 2003 and 2006 pilot schemes the Council decided to pilot further e-voting in the May 2007 elections.

2.3 In order to comply with their statutory requirement to evaluate pilots, the Electoral Commission (the Commission), appointed Actica Consulting Ltd (Actica) to conduct the technical aspects of the electronic voting evaluations. Actica has evaluated the e-voting pilots to provide an:

a. assessment of the degree to which the suppliers have met the requirements of the pilot;

b. analysis of how effective the system was in practice, including accuracy, reliability, robustness, security and functionality aspects;

c. assessment of the risks to the effectiveness of the system;

d. analysis of the adequacy of the development lifecycle, covering project management, risk management, requirements, design, implementation, deployment and testing;

e. analysis of the testing process including accuracy, reliability, robustness, security and performance tests;

f. analysis of the effectiveness of the Quality Assurance (QA) processes performed, together with analysis of the actions taken by suppliers as a result of the QA process commissioned by the Ministry of Justice (MoJ);

g. assessment of any other technical issues that may have affected the success of the local election;

h. assessment of the extent to which the desired technical learning outcomes of the pilot were met and whether any other learning points were developed during the pilot.

2.4 To complete this required analysis and assessment Actica produced an evaluation framework, and agreed its content with the Commission. The framework provides a description of the overall evaluation process and approach that was used as the basis of the technical evaluation for all e-voting pilots. It describes the information sources that were used during the evaluation, the structure of the content of this report and provides comprehensive guidance on questions that should be answered. The full content of the framework can be found on the Commission website.

2.5 Following the guidelines of the framework, the remaining sections of this report for the technical evaluation of the Council e-voting pilot are structured as follows:

a. **Section 3 – Pilot objectives**, which describes the overall objectives of the pilot including the measures by which success is judged;

b. **Section 4 – Pilot description**, which provides a high-level description of the pilot;

c. **Section 5 – Management**, which describes the management of the pilot, including project management, relationship management, risk and contingency management quality management, testing, training and support provided;

d. **Section 6 – Technology**, which provides a high level technical description of the pilot system;

e. **Section 7 – Security**, which describes the key security issues associated;

f. **Section 8 – Cost**, which describes the cost of the election and relates to the benefits and overall value for money;

g. **Section 9 – Conclusions**, which summarises the key points identified in the report.

3 Pilot objectives

3.1 Objectives

3.1.1 The objectives of the pilot scheme were to[1]:

a. increase voter choice;

b. increase voter turnout by increasing the opportunities to vote and to raise awareness;

c. improve security;

d. build confidence through the use of new technology applications to increase support for the use of such systems;

e. facilitate voting amongst hard to reach groups through the flexibility and accessibility of the system to assist specific categories of voters (e.g. service personnel and foreign nationals);

f. assess the practicality of integration of the e-voting channel with existing electoral systems and processes.

3.1.2 The technical aspects of whether these objectives were achieved are considered within this report.

3.2 Success criteria

3.2.1 The specific outcomes that were set by the Council for the pilot were:

a. to increase the number of people voting by 5%;

b. to reduce the time taken to undertake the count and the resources required to complete the count process;

c. for 20% of the total votes cast at the election to be from electors voting via the internet;

d. to determine whether the number of residents who indicated through consultation that they would use the internet, are reflected in the results;

e. to ensure high levels of trust and confidence in the system (as assessed from an analysis of completed questionnaires provided as part of the e-voting process);

f. to increase awareness of the voting process especially amongst hard to reach groups (e.g. armed forces personnel).

3.2.2 The last of these objectives is not within the scope of the technical evaluation and is not considered further in this report. It is however considered in the Commission's overall assessment of the pilot.

---

[1] Electoral Modernisation Programme, November 2007 Electoral Pilots Application Form from Rushmoor Borough Council.

INTENTIONALLY BLANK

4 Pilot description

4.1 Introduction

4.1.1 The Council piloted remote voting via the internet during the week before polling day and on polling day itself. Postal voting, proxy voting and voting at polling stations were also available to the electorate, as at normal local elections.

4.1.2 The pilot included:

a. registration and use of personal identifiers for e-voting;

b. e-enabled voting from any location.

4.1.3 Unlike the other four e-voting pilot schemes, the Council had decided not to pilot the use of telephone voting. This was because its previous experience during the 2003 election had suggested that there was little interest within the borough in telephone voting.

4.2 Registration

4.2.1 Electors were required to pre-register if they wished to vote via the internet. Pre-registration for internet voting was initially intended to be undertaken on-line. Following discussions between MoJ and the Council a paper-based registration process was agreed. This was to reduce the risk of fraudulent registration.

4.2.2 Registration involved the following:

a. Letters were sent to all registered electors informing them that they could vote via the internet. Included with the letters was a registration form. The registration form was also available for download from the Council's web site.

b. Electors were required to complete the registration form and return it to the Council by the 18th April. The registration form required the elector to provide a 6 to 10 character username and their date of birth. They were also required to sign the form.

c. Registration was undertaken by the Council staff. This included manual input of elector details, recording the username and date of birth, marking the elector as an internet voter, validating the signature provided on the registration form where possible and resolving any queries that arose.

d. A letter was sent to the electors to confirm that they had been registered to vote electronically.

e. The registration information was sent in a password protected zip archive file (containing a CSV file) to ES&S (the supplier).

f. The supplier produced a set of unique Voter Identification Numbers (VINs).

g. Registered electors were sent a security sealed internet poll card that contained their VIN (but not their username or date of birth). For multiple occupancy buildings the poll cards were hand delivered.

4.3 E-enabled voting

4.3.1 The internet voting period commenced at 6.00am on Thursday 26th April and ended at close of poll at 10.00pm on Thursday 3rd May. The elector was required to provide their username, date of birth and VIN before they were able to vote. The system validated their identity and confirmed that they had not already voted. A ballot paper, for the ward the elector was registered in, was then presented to the elector. The elector selected who they wished to vote for, the vote was cast and a receipt was provided to the elector as confirmation that their vote had been cast.

4.3.2 A registered e-voter was able to change their mind prior to voting and choose to vote at a polling station. To do so they had to prove their identity at the polling station. The election official would contact by telephone the Call Centre (staffed by the Council's Electoral Services team) who would confirm that they had not voted electronically. The electronic vote was then cancelled and the elector was issued a paper ballot.

4.3.3 After the polls closed, the electronic ballot box was downloaded to a PC within the count centre. The ballot box was unlocked and the votes cast were verified. This was performed in parallel with the process of verifying all the ballot boxes. Once verification was completed the ballots were counted (again in parallel with the manual count). These results were added to the traditional and postal results. Candidates were presented with the results (including the split of votes between the internet and traditional vote). After it was confirmed that a recount was not required, the presiding officer declared the results. Note that a process was in place to perform a complete recount of the electronic ballots if this had been required.

5 Management

5.1 Introduction

5.1.1 The pilot was run by the Council's Electoral Services department. The e-voting system supplier was ES&S who were supported by:

a. Intelivote – provider of the voting front end;

b. Scytl – provider of the electronic ballot and vote sealing software;

c. FirstServ – provider of the internet hosting facilities.

5.2 Project management

5.2.1 A joint council / supplier Project Team was established and the project was managed using a project management methodology based on PRINCE2.

5.2.2 The Council appointed a senior member of staff to act as the overall project sponsor. The project sponsor (the Council's Head of Democratic Services) had substantial experience of electoral modernisation pilots. He had taken a leading role in the 2003 and 2006 pilots performed by the Council. The sponsor took an active role in directing the project. He was supported by an overall pilot Project Manager who was also a Council employee (Corporate Projects Officer).

5.2.3 The Supplier appointed a Project Manager who took responsibility for the delivery of the electronic system. The Supplier's Project Manager also managed the South Bucks pilot[2] that shared some infrastructure with the Council's pilot[3]. Each of the Supplier's sub-contractors also identified a Project Lead. The leads fulfilled a similar role for the South Bucks' pilot. It should be noted that during the bidding process the South Bucks' pilot and the Council's pilot were treated as separate assignments. The projects were therefore treated as separate (but strongly interdependent) projects by the supplier with separate documentation produced for each but with a significant number of the key staff and key resources being common to both projects. Given the short timescales associated with the pilots, the use of a common staff increased the risks to the Council pilot due to potential resource conflicts within the supplier team. It is also noted that the use of the shared infrastructure reduced the time available to perform the Council's pilot because of the need to complete all testing prior to the South Bucks e-voting election starting on 21st April.

5.2.4 The exact division of responsibility between the Council and the Supplier was not clearly defined initially and, in response to the MoJ QA audit, a memorandum of understanding (MoU) detailing these responsibilities was produced.

---

2 The South Bucks e-voting pilot shared the same supplier and broadly the same technology as the Rushmoor pilot.

3 The supplier reported that this was done at the urging of MoJ during the Best and Final Offer period to provide efficiency savings.

5.2.5 The Council maintained an overarching project plan for the pilot scheme which included key technical milestones and an overall risk register. The supplier maintained a separate detailed project plan and risk / issue register that considered only the technical aspects of the pilot scheme. The project plan and risk register were reviewed at regular weekly checkpoint meetings or teleconferences. Highlight reports and minutes of the meetings were produced. The Council's project sponsor commented that there would have been value in the Council and supplier having a single integrated project plan.

5.2.6 Whilst the roles defined and overall approach to project management were sensible, there were a number of shortfalls in the Supplier's project and quality management arrangements, namely:

a. adequate project documentation was not maintained;

b. quality, testing and acceptance procedures were not adequate.

5.2.7 Discussions with the supplier suggested that these shortfalls were due to the tight timescale for the pilot. In our discussions with the supplier, it was stated that around six months are required to properly implement a pilot of this scale. In this case the MoJ Framework contract was not let until 10 January, the invitation to tender for the pilot had was not issued until 15 January and approval to proceed with the pilot was not finally received until late February. This means that the time available was limited to less than 3 months, and the Supplier's effort during this period was split between Rushmoor and South Bucks. As such, the problems encountered were entirely predictable and should not be seen as reflecting adversely on the supplier. Rather they are indicative of poor procurement practice within the MoJ – it is strongly recommended that pilots are not undertaken unless Suppliers can be given the required time from contractual approval to proceed to the start of the voting period, since otherwise the risk of failure and resulting loss of confidence in e-voting is too high. The timings of local elections are known well in advance, so there can be no sensible reason for not planning sufficiently in advance to ensure that pilots can be undertaken with a low level of risk.

5.2.8 It is also noted that the pilot was treated as a short project run to very tight timescales. It was not managed as a longer term 'programme' that would enable the more effective integration of internet voting into the Council's election processes. This also reduced the ability of the Council to recoup benefit from the investment made in the development activity.

5.3 Relationship management

5.3.1 The relationship between the Supplier and the Council appeared to work well in general. The relationship between the different members of the Supplier organisation also appeared to work well. Minor difficulties were experienced due to the geographic spread of the team during the early stages of the project. Elements of the team were located in England, Spain, the USA and Canada. Earlier co-location of the team may have been beneficial.

5.3.2 A high level Statement of Requirement (SoR) for the pilot was developed by the Council. It was produced in a short period of time (only a few days were allowed for it in the MoJ timetable) and the author of the SoR was unaware of the more detailed requirements with which the Supplier was required to comply as a result of the framework contract. Some aspects of the requirement were defined at a high level only, and the requirements evolved as the pilots progressed, for example responsibilities for providing the call centre were not finally clarified until 4 weeks before the election.

5.3.3 Two bids for performing the pilot were received. The Council selected their preferred supplier. In discussion, the Council's project sponsor noted that he had been disappointed that it had

proved difficult to compare the costs obtained from the two bids received despite the existence of a common framework contract. MoJ may wish to review this before holding future pilots. Once the Council had selected their preferred supplier MoJ held on-going negotiations with this supplier to agree savings as a result of the supplier performing two pilots.

5.3.4 Discussions with the Council's Project Sponsor suggested that he did not have a detailed understanding of how the framework contract worked nor of the contractual relationship with the supplier. Without a clear understanding of the contractual relationship effective commercial management of the contract cannot be achieved.

5.3.5 The relationship between the MoJ and the Council could be significantly improved. The MoJ for example, could in the future ensure that the Council:

a. has a good understanding of the overall strategic direction of the Electoral Modernisation programme and how a particular pilot fitted into the overall programme;

b. is aware of the lessons that have been learned from earlier pilots;

c. has a good understanding of the framework contract, the results of their evaluation of the suppliers bids to get on to the framework and any particular issues or concerns as a result of the evaluation;

d. has a good understanding of the requirements placed on the supplier as a result of the framework contract.

5.3.6 Delays in initiating the project and providing final approval to proceed added to the risks associated with the pilot. Changes in the boundaries of the project added further risk to the project. Delay of the QA activities until just prior to the election meant that there was very limited opportunity for remedial work to be performed. An on-going QA activity through the project lifecycle would be more effective. Some QA activities should have been performed prior to the pilot commencing.

5.4 Risk and contingency management

5.4.1 The Council adopted a standard approach to risk management. An overall project risk register was produced that held details of each identified risk, the probability of the risk occurring, the mitigation action to be taken and the owner of the risk. The risk register was reviewed at weekly checkpoint meetings. The Supplier followed a similar approach.

5.4.2 The main technical risk that occurred for the council was associated with the Council's Election Management System (EMS). This system needed to be 'patched' to enable internet voting details to be recorded. Substantial delays occurred in obtaining the required patch from Pickwick (the EMS supplier). A fallback plan was developed that involved the Council directly entering the information into the Intelivote system. In the end the patch arrived just in time so that the contingency measure did not need to be invoked.

5.4.3 The Supplier had included substantial redundancy within their system design. No availability issues with the Supplier system emerged during the election period. While some electors did experience availability issues, it is understood that these were associated with the Council's website, which provided a link through to the voting website. Electoral administration staff within the Council also encountered minor availability issues with accessing the main voting administration functions. These were traced to problems with the Council's internal IT system rather than the Supplier's system and had no significant impact on the ability of the Council to manage the election.

5.4.4 The security risk assessment performed by the Supplier was superficial; it was based on the Supplier's experience. A systematic risk assessment approach was not performed. Residual risks that the Returning Officer accepted in proceeding with the pilot were not identified. An adequate Risk Management and Accreditation Document Set was not produced. Without this information an independent assessment of the technical, procedural and personnel security measures cannot be determined. The lack of such an independent assessment must be seen as reducing the level of confidence in the security of the system.

5.5 Quality management and testing

5.5.1 A high level quality plan was produced for the pilot by the Council. This covered the activities that the Council performed.

5.5.2 An acceptable quality plan was not produced by the supplier. A number of other key project documents were not provided by the Supplier to the Evaluator and it is therefore assumed that it was not produced. This included:

a. detailed design documentation;

b. test plans;

c. quality records (included the results of reviews and detailed test results).

5.5.3 No evidence was provided by the Supplier that design reviews or code reviews had been performed. No evidence was provided that the Supplier had taken a systematic approach to testing.

5.5.4 A high level summary of the tests that had been performed was provided. This indicated that:

a. high level installation tests were performed (e.g. to confirm that the system failed over correctly);

b. checks of the links between screens, functioning of buttons, names of candidates and parties on the ballots, generation of output data, etc. were performed (although it is noted that an error in a party name was not picked up as part of the tests despite the test having been recorded as having been passed);

c. checks of the key generation[4] functionality were carried out;

d. basic end to end system tests were undertaken once installed at the hosting environment.

5.5.5 No evidence was provided to enable confirmation that the supplier had an acceptable configuration management process in place. Details of the version of the system tested, the test scripts used, and the regression tests performed as a result of test failures were not provided.

5.5.6 No evidence was provided that the supplier had performed stress testing of their system.

5.5.7 FirstServ (the Internet hosting provider), performed a vulnerability scan of the system. This identified 5 potentially critical security vulnerabilities, 20 potential serious vulnerabilities and a large number of more minor and actual vulnerabilities. This test was performed in parallel with the independent external penetration testing (see Para 5.5.9). The value of the vulnerability scan performed by FirstServ was reduced because of the timing of the work. It would have been

[4] The key generation functionality is used to produce a public/private key pair that is used to lock the ballot box during the election. See Section 6 for more detail.

beneficial for the scan and any required remedial work to have been performed prior to the independent penetration test. This would allow the independent penetration test to confirm that the required remedial work had been correctly performed.

5.5.8 The Council produced an acceptance test plan. This test plan covered major elements of the functionality provided by the e-voting system. It included holding a mock election in which 599 ballots were cast by the Council's staff. The results were verified against the results generated by the system. The acceptance tests, while covering the major elements, were not comprehensive. The full set of requirements in the SoR / framework contract was not tested. The full functionality of the system was not tested. For example, the issuing of replacement VINs and the impact that this may have on the overall count was not tested (see paragraph 6.2.12). Possible failure modes while voting were also not explicitly tested. The counting report generation was not tested. The short timescales available for testing limited the set of tests that the council could perform. The Council's Project Sponsor noted that he had not been able to perform some of the acceptance tests he had planned to perform. It is essential that sufficient time is allowed for full acceptance testing to be performed as part of the process of planning a pilot.

5.5.9 An external 'black box' penetration test was performed for the MoJ by MWR Infosecurity (a CESG CHECK Green light supplier[5]). This identified 2 high risks, 2 medium risks and 7 low risks. Though the supplier stated they had updated the system to address a number of the weaknesses found, they were not able to respond to all the concerns raised due to the fact that some changes would have required a reinstallation of the system and there was insufficient time before the system was due to be live. It is also noted that the MWR Infosecurity representative commented in his report that insufficient time had been allowed for the penetration testing and that he was therefore unable to guarantee that this was thorough and complete.

5.5.10 It is recommended that a full IT Health Check is performed as part of the evaluation of internet voting systems prior to the election. This includes 'white box' and internal penetration testing. Sufficient time for this health check to be performed thoroughly must be allowed. Time for any required remedial action must also be allowed for when planning a pilot.

5.5.11 As previously noted by the Commission, an accreditation / evaluation of key system components prior to the election is also recommended. This would enable a detailed assessment of their correct implementation to be confirmed and any vulnerabilities identified to be remedied.

5.5.12 The MoJ commissioned an independent quality audit from Security and Standards Ltd. The QA involved:

a. an initial meeting with all the pilot technology suppliers to explain the approach to be followed to the QA assessment;

b. a telephone interview with the supplier;

c. review of documentation provided;

d. further face to face discussions with the supplier and local authority representatives at the Council's offices.

---

55 CESG is Her Majesty's Government Information Security Technical Authority. CESG operate the CHECK scheme. This scheme assesses suppliers of IT health check (penetration testing) services to ensure the quality of the service they provide. Details of the scheme and the evaluated suppliers may be found on the CESG website (www.cesg.gov.uk).

5.5.13 The audit focused on the security elements of the system. It involved a structured set of questions organised around the controls identified in ISO/IEC 17799[6]. While the supplier provided acceptable answers to the main questions, the QA representative was only able to obtain limited confidence that there were no unacceptable residual risks with the pilot due to the limited supporting evidence presented by the supplier.

5.5.14 Although a number of useful recommendations were identified by the QA representatives, the true value of the audit was limited because it was performed so close to the election and therefore provided limited opportunity for corrective action to be taken. It is strongly recommended that independent QA / technical assurance activities are performed throughout the pilot project and are not delayed to two days before the election is due to commence. This would enable problems to be identified much earlier and appropriate remedial action taken. There would also have been merit in the audit including a visit to the hosting location.

5.5.15 It is also noted that some of the required QA activities could be performed prior to the start of the pilot project. For example, the detailed quality management, configuration management and testing approaches to be followed could have been defined in the suppliers bid for the pilot and assessed prior to the award of the contract.

5.6 Training

5.6.1 Two types of tailored training and associated material were delivered by the supplier:

a. **Call centre staff** were provided with an overview of the e-voting system and specific training in the ability to determine whether a voter contacting the call centre had registered to vote electronically, how to cancel VINs, how to issue new VINs and the approach to be followed if users had forgot their usernames.

b. **Electoral Services staff** involved in the overall administration of the election were provided with further training on the use of the administrative console that provided them with the ability to monitor the election.

5.6.2 Training involved direct one–to-one instruction in the use of the system. A user guide was also provided. No issues were identified in respect of the training, and feedback suggested that the Intelivote election management applications were found to be simple to use.

5.7 Support

5.7.1 The e-voting system was operational for seven days and during this period support was provided by a call centre comprising the Council's staff and two employees from Intelivote. A central helpline number was included in the information provided to electors. This helpline could provide assistance to voters who did not know if they were registered to vote electronically, who had forgotten their Voter Identification Number (VIN) or username, or who wanted to know whether their vote had been successfully cast. Staff had the ability to modify voter details (e.g. reissue a VIN or provide hints to enable an elector to remember their username. The Intelivote system provided tools to support them in resolving queries. Feedback from the Council suggests that this was generally easy to use. It was noted however that it would have been beneficial to enable logging of query types within the tool.

---

[6] ISO/IEC 17799 is an international standard that provides a code of practice for information security management.

5.7.2 The status of the e-voting system was monitored in several ways throughout the period of operation:

a. the hosting provider monitored standard technical characteristics (e.g. memory usage). The ES&S system manager was notified automatically (by SMS) if their performance moved outside agreed boundaries;

b. the ES&S system manager periodically reviewed the system logs to review the level of use of the system and to look for any unusual activity (e.g. a high number of unsuccessful access attempts).

5.7.3 Call centre staff were also instructed to pass on any reports of system unavailability or abnormal operation onto the ES&S system manager. No significant availability issues occurred. The Project Sponsor noted that to start with, users who were voting from a local library had difficulties because the library's firewall blocked active content. Arrangements to remedy this had to be made. (It is noted that the terminals used in the Library were not supplied specifically to support the election).

INTENTIONALLY BLANK

6 Technology

6.1 Registration process

6.1.1 The registration process for the e-voting solution was managed by the Council and required electors to opt-in to voting via the internet. An application form was posted to every registered elector and was also available to download on the Council website.

6.1.2 As part of their application to utilise the e-voting channel, electors were required to provide a 6 to 10 character username and their date of birth (DoB). The username and DoB provided a weak password for the system. The username and DoB were not documented in any subsequent communications from the Council and were to be kept in a safe place by the elector. The elector was required to sign the application form. The signatures were manually compared to those held by the local authority. The Council's Electoral Service staff resolved the small number of issues identified through contacting the relevant electors.

6.1.3 The registration system information was captured in the Council's Election Management System. This system was provided by Northgate Information Systems (Pickwick). Before the information could be entered into the system a patch was required. There were delays in obtaining the required patch. Although the patches were eventually received, these delays had a knock on impact on the project and overtime work was required to keep the project on track.

6.1.4 A number of difficulties with the patched registration system remained. For example, it was reported that it was difficult to validate that a voter had been issued one vote only. The Council had to perform a manual check of the marked up register to confirm that no one had been issued both a postal and internet vote.

6.1.5 The registration process resulted in approximately 200 to 300 queries during the verification process. These were mainly associated with incomplete registration forms. A number of people did however, eventually decide to vote in person having registered for internet voting. Their reasons included the fact that they had registered in error, or because they experienced difficulties with the internet voting solution.

6.1.6 The register of electronic voters (including details of the username and date of birth) was exported from the Pickwick system and issued to the Supplier. The Supplier generated a set of eight digit voter identification numbers.

6.1.7 Each elector was notified of their unique VIN by post in a secure mailer that also served as the official poll card. For electors in multi-dwelling locations the secure mailers were hand delivered. The secure mailer was designed to prevent the VIN from being read without opening it, opening of the mailer required tear-off strips to be removed clearly indicating if it had been tampered with. If an elector did not receive their VIN they could contact the Council to request a new number to be issued. ES&S arranged for the printing of the VINs using the printer recommended by the Council. This printer had been used on a number of occasions by the Council, which regarded the company as reliable.

6.1.8 A number of spare VINs were generated. These acted as a reserve pool that could be drawn on in the event that an elector lost their VIN. If this occurred the Council help desk staff would

confirm that the elector had not already voted, cancel the lost VIN and deliver a new VIN to the elector.

6.1.9 Contest information was also captured in the Council's Election Management System. This was exported as a PDF file which was issued to the e-voting system supplier.

6.1.10 Verification of the information on the election system was implemented through a manual check. One error went undetected until the first day of voting. A candidate was given the wrong party emblem and their party name was misspelt. This was picked up at a very early stage in the election and was rapidly corrected (only one vote had been cast before the error was corrected).

6.2 Voting process

6.2.1 Once the e-voting system was 'live', an elector could cast their vote at any time during the operational period.

6.2.2 As part of the process by which an elector cast their vote over the internet, e-voters were required to:

a. **access the voting web site** by entering the HTTPS address provided on the official poll card in their browser or clicking on the hyperlink provided on the Council's website. The system required the elector to have a PC with an internet connection (dialup or broadband connections were suitable) running Internet Explorer (version 6 or higher) or Mozilla Firefox (version 1.5 or higher). It was confirmed during the testing process that the Safari web browser could also be used.

b. **enter the randomly generated security code** that was displayed as an image on the screen in the required box. Alternatively a downloadable audio message could be obtained. This step was designed to inhibit automated attempts to access the system.

c. **enter the VIN provided** in the official poll card and corresponding username and date of birth selected previously by the elector. This information was verified against the records held by the system. Further checks were made to identify if the elector had already cast their vote and to determine in which ward the elector was entitled to vote. The elector had five opportunities to enter the correct VIN, username and date of birth combination before their profile was locked, requiring them to contact the call centre.

d. **review the ballot paper presented** on screen and select who to vote for. Selections were made by clicking on the name of the candidate using the mouse. The ballot paper was presented in the same format as a standard ballot paper. The system did not allow overvoting. A blank vote could however be cast, 44 of which were cast during the election.

e. **submit the completed ballot paper**. If the elector wished to change the selection it could be done prior to the vote being submitted. Once the elector was satisfied that the selection had been recorded correctly he/she could choose to cast their vote. Once this step had been completed the selection could not be changed.

6.2.3 A unique receipt number was then presented on screen. This provides a link to the ballot cast and the elector was instructed to make a note of it. The provision of this receipt confirmed that the ballot had been successfully recorded by the system in the eBallot Box. Details of how the receipt was generated are provided in paragraph 6.3.14. The receipt was also stored in the ballot box. It should be noted that the receipt does not provide details of who the ballot was cast for. The Council have recently published the list of receipts from the opened ballot box on their web

site[7]. It is too soon to determine how many people actual take advantage of this to confirm that their vote was counted. It is noted that the Council has not decided not to actively publicise the fact that the list is now available on-line due to their concerns over its usability.

6.2.4 If an elector forgot their VIN, username or date of birth, he/she could contact the call centre for assistance. There were 591 calls to the help desk, the vast majority of these calls were associated with people having forgotten their usernames. If an elector was able to provide their VIN and date of birth the call centre staff would give up to two characters of the username. If the elector still was unsure of their username this would be hand delivered by the Returning Officer's staff. They required the elector to validate their identity before handing over the user name.

6.2.5 If a user forgot their VIN and had not voted, their old VIN was cancelled and a new VIN issued. Alternatively if they had not voted already they could choose to vote at their local polling station.

6.2.6 Of the 6,686 people who registered for e-voting only 4,157 (about 62%) attempted to vote using the Internet channel. 186 finally choose to vote at a polling station (3%). Of those who attempted to vote only 3,827 (92%) successfully cast their vote. Approximately 315 voters failed to cast a vote and did not contact the help desk to resolve their issue . Anecdotal information obtained from the Council's Project Sponsor suggested that the voters, having initially failed to log on successfully were not sufficiently well motivated to incur the additional inconvenience of contacting the call centre to resolve the problem.

6.2.7 Tendered and proxy votes were not supported on the e-voting channel.

6.2.8 It is noted that the management system enabled electoral officials to track who had voted and when they voted. This information may be of interest to political parties as it would enable them to target their campaigning. It is understood that it is not however, currently legal to provide this information prior to the close of the poll.

6.2.9 Each polling station was issued with a list of electors who had registered to vote via the internet. If one of these electors tried to vote in a polling station, the electoral officials would contact the Electoral Administration staff via the telephone and check that the elector had not already voted on line. If the elector had not voted, their internet vote was cancelled and a paper ballot was issued.

6.2.10 Once the poll had closed, the contents of the eBallot Box were downloaded from the hosting provider to a PC at the counting centre over a secure Virtual Private Network (VPN) connection. The contents were then copied to a CD and transferred to a separate PC without network connectivity. The eBallot Box was then opened. Ballot results and receipts were then exported onto CD and passed to a separate machine for counting. The opening of the ballots and mixing of the associated receipts was a process managed by Scytl technical staff and required detailed knowledge of the software to complete (e.g. command line processing of software functions). Details of the process are described in the next section. A more automated process subject to independent validation would be desirable.

6.2.11 In the case of a judicial review of an election it would be possible to link the result in a particular ballot to the elector who cast the vote by extracting a ballot from the eBallot Box prior to decryption and decrypting it individually to determine its result. This would require the

[7] http://www.rushmoor.gov.uk/media/adobepdf/s/m/iVote_Receipts.pdf

voter's unique VIN to be determined and linked to the related receipt which is attached to each encrypted ballot. A copy of the eBallot box in its encrypted state was archived by the Council in case such a step was required in the future. It is to be kept for the required Statutory Period.

6.2.12 The counting process was performed in two steps. The first step involved counting the number of receipts in the eBallot box for each ward and comparing this to the record of the number of ballots cast for each ward as determined from the vote collection system (see Section 6.3). Once the verification process had been completed the votes were counted. However, the import of e-voting results into the vote tallying application (see section 6.3) identified errors in the underlying data records for a small number of ballots. These errors prevented the import of any e-voting results until the issue was resolved. The reason for the errors was a blank data field (the ward identifier) in a number of records, eventually traced to an issue with the process of reissuing a VIN to an elector. Once the reason for the error was identified the affected ballots were modified manually before the import process could continue. Though this introduced only a small delay to the process it does raise a number of concerns; firstly, that these errors were not picked up during testing and were not identified until count night. Additionally a number of printer problems were encountered on the night. This too slowed down the ballot verification and results generation process. These issues should have been resolved through prior testing. The total delay caused by this and the issue identified in paragraph 6.2.12 was of order ½ hour.

6.2.13 A process for performing a complete recount was defined. This involved cleaning all the tallying PCs of ballot information and downloading and reopening the ballot box. This was not needed.

6.2.14 The candidates and agents were kept informed on progress during the count through a rolling PowerPoint® presentation.

6.3 Technical architecture

6.3.1 The three main elements of the e-voting system were:

a. **Infrastructure** - this was provided by the hosting provider. It consisted of firewalls, context sensitive routers, servers, power distribution units and tape backup facilities.

b. **Vote collection system** - this comprised:

1. **Internet voting interface** - this provided the interface between the voter and election system. It included the functionality required to present the ballots to the voter and sent the cast ballots to the electronic ballot box. It consisted of three types of server, namely voting interface application servers, voting interface infrastructure servers and voting interface database servers. There were two active servers of each type and one stand by.

2. **eBallot box** – this provided the application that supported the casting of the votes, production of ballot receipts and the storage of the encrypted cast ballots in the electronic ballot box. It consisted of two ballot casting application servers and two ballot casting database servers. The ballot box application contained Scytl's pnyx.core voting service application.

c. **Vote tallying** – this consisted of a number of PCs that were used to tally the votes. One of these PCs contained Scytl's pnyx.core mixing service, another contained ES&S's application that counted the cast ballots.

6.3.2 The physical components of the infrastructure and vote collection system were shared with the pilot run by South Bucks. They were hosted at the FirstServ data centre. FirstServ provided

physical protection of the hosting environment (e.g. rooms were reported to be locked with entry by digital keycard, and there was constant surveillance, CCTV in all receptions and hallways and security zones using alarms and card access). The environment was equipped with climate control and fire protection facilities. A security audit of the location was not performed by the author of this report or the MoJ QA representative.

6.3.3 ES&S stated that FirstServ staff only had the ability to reboot the servers supporting the e-voting solution. Once installation had been completed the applications were locked and all further administration was completed remotely by Intelivote and Scytl via a VPN that encrypted all data when in transit. The security controls in place to ensure that only ES&S staff had access to the system were not documented. Use of the VPN required a user to have a valid security certificate on their client PC as well as a valid username and password. These security credentials were only available to the ES&S system manager and authorised members of his technical support team and were used from dedicated laptops. The technical, physical and procedural controls in place to protect these machines were not documented.

6.3.4 The system had a high level of redundancy including:

a. redundant servers;

b. redundant firewalls;

c. redundant switches;

d. redundant power supplies;

e. multiple connections to the internet.

6.3.5 It is likely that the service would only have been disrupted in the event of a major disaster at the hosting facility.

6.3.6 The technical solution included remote backups taken at daily intervals throughout the voting period. Backup tapes were stored off-site in a fireproof safe. The measures to protect the tapes and the data on them were not documented. A high level business continuity plan had been prepared and tested through a structured walk through.

6.3.7 ES&S stated that they would usually scale an e-voting solution to support double the expected scale of the election. The minimum level of hardware required to provide the level of redundancy far exceeds the capacity required of the combined Rushmoor and South Bucks pilots. The supplier estimated that the system was capable of supporting 100 times as many votes as registered in the two elections. No actual stress testing was performed so validation of this claim is not possible.

6.3.8 Detailed design documentation was not provided. This prevented confirmation that firewalls, servers and switches had been configured in accordance with best practice. The high level description suggested that the system was configured in a standard manner. While not mentioned in the high level design documentation it is also understood that an Intrusion Detection service and a service providing mitigation against distributed denial of service attacks were procured from FirstServ.

6.3.9 The Pnyx.core application provides a set of software components that were integrated into the Intelivote voting system. A high level overview of how the Pnyx application works is provided below.

6.3.10 As noted in paragraph 6.3.1 and illustrated in Figure 1, the internet voting system can be considered to be composed of three components:

a. The client PC that is used to access the voting system.

b. The vote collection system that is used to collect the votes received over the internet.

c. The vote tallying system receives the votes from the vote collection server and tallies these votes to obtain the results. For the pilot the vote tallying service was not connected to the internet.

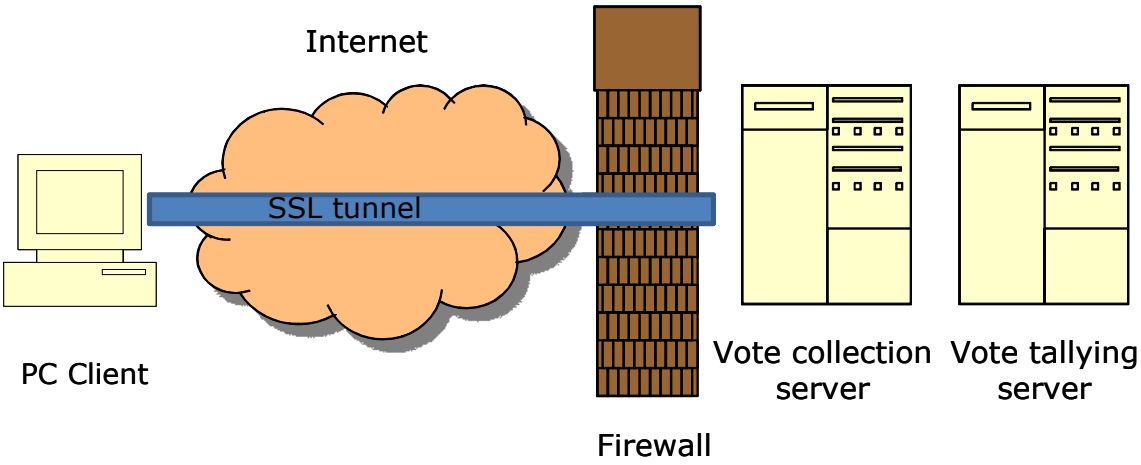

Figure 1 – High level representation of the components of an e-voting system

6.3.11 Pnyx consists of three components:

a. Mixing service;

b. Voting service;

c. Voting client.

6.3.12 The **mixing service** resided on the vote tallying system (a Scytl owned laptop). This vote tallying system was air gapped from the internet. The first task that the mixing service performed was to generate a public / private key pair for a particular election. The public key was used during the election to encrypt ballots; the private key is required to decrypt the ballots. A public / private key pair was generated on the laptop. Once the public private key pair had been generated the private key was broken by the mixing service and distributed across three smart cards. Each smart card was protected with a username and password. These smart cards were issued to the Returning Officer, the project sponsor and a key member of his Project Team. These three people are referred to as the Electoral Board. To be able to reform the private key any two of the three smart cards were required.

6.3.13 The **voting service** resided on Intelivote's vote collection server. It handled the voting protocol with the **voting client**. The voter accessed the election web page over an encrypted (SSL) link. The **voting client** is an applet that was downloaded to the voter's browser. The voting client asked the voter for their voting credentials (username, date of birth and VIN). This was passed back to the voting service. The voting service generated a public / private key pair for the client. The key pair was then downloaded to the client. A personalised ballot was then sent from the vote collection server to the client. This ballot was encrypted with the client's public key.

6.3.14 The voter then made his choice of which candidate to vote for using the voting client applet. The voting client generated the contents for a voting receipt. The completed vote and the contents of the voting receipt were sealed (encrypted) in a digital envelope using the election public key. This envelope was signed with the client's key. The voting client prepared a voting receipt validation request for validation by the voting service. The voting receipt validation request and the signed digital envelope containing the vote were then sent over the SSL connection to the voting service.

6.3.15 The voting service confirmed receipt of a valid digital envelope. Having done so it validated the voting receipt. The voting receipt was then passed back over the SSL link to the voting client which displayed it for the voter so they could make a note of it. The voter can use this receipt later to confirm that his/her vote has been counted. It does not however, provide any information of who the vote was cast for.

6.3.16 This process was repeated for each voter. The votes were stored in their digital envelopes on the voting service until the close of the election. They were then transferred to the vote tallying machine. This occurred through the administration team remotely logging on to the server (see paragraph 6.2.10).

6.3.17 The Electoral Board reconvened. The private key was reformed by the mixing service from the information held on the smart cards. The digital envelopes were then opened and the votes, voting receipts and the voters disassociated. The voting receipts and the cast votes were then sent to the tallying application for counting. Further details of the protocols used may be found at http://www.scytl.com/docs/pub/science/PNYXCOREWhitePaper.pdf.

6.4 Use of EML

6.4.1 EML was not used to exchange information between the election voting system and the election management system operated by the Council. Candidate details were provided in a PDF file. Electors details were provided as a CSV file. EML was claimed to be used by the Supplier internally to the system. Conformance testing to verify this was not performed.

INTENTIONALLY BLANK

7 Security

7.1 Security of the voting system

7.1.1 The supplier did not perform an adequate systematic security risk assessment. A high level risk assessment based on their general experience was performed. The supplier claimed that there had been insufficient time to allow a more detailed assessment to be performed. Failure to perform a thorough risk assessment is considered a major shortfall. It is strongly recommended that a thorough risk assessment is performed for all pilots.

7.1.2 The required Risk Management and Accreditation Document Set (RMADS) was not provided. An RMADS is a key security document. Its content includes details of the scope of the system, the assets that comprise the system, the security responsibilities, the threats to the system, the vulnerabilities of the systems, the risks to the system, the countermeasures (including, technical, procedural, personnel and physical measures), the residual risks, the security procedures, the results of the security testing performed and plans for any further testing it is proposed to perform. It provides a substantial body of evidence that an acceptable set of security measures are in place and a basis for an independent security audit. It is considered a significant failing that this document was not provided.

7.1.3 The MoJ QA activity included a review against the controls identified in ISO/IEC 17799. The MoJ QA auditor found that to some extent measures were either in place, or were going to be put in place, addressing each item / control in the auditors pro forma. Where there was an issue outstanding there was an agreed resolution to that issue between the supplier / local authority and the auditor, this gave the auditor sufficient comfort that the major risks had in fact been identified and controls put in place. In the author's opinion this does not provide an adequate level of assurance and a more systematic and rigorous approach is required. Any supplier who does not have a sufficient understanding of security to be able to produce an acceptable RMADS should not be used in e-voting pilots. It is recommended that an outline RMADS should be requested as part of the bidding process for future pilot elections. Assessment of this RMADS should form an important element of the bid assessment process.

7.1.4 The MoJ commissioned an independent penetration test of the system; only black box penetration testing was performed. The timescales for performing the penetration testing were too short and insufficient time was allowed for remedial action to be taken. Independent penetration testing is a critical activity in providing assurance of the security of the central voting infrastructure. A full Health Check including both internal and external white box penetration testing by an independent CESG Check approved supplier (or CESG) should be performed for all internet voting pilots.

7.1.5 A number of security innovations were piloted. These included a more rigorous approach to e-voting registration and the use of the pnyx.core e-voting security suite. Whilst the registration process caused difficulties with usernames being forgotten, the requirement for signed registration forms that can be checked against the previous records (where available) is seen as a useful measure in reducing the risk of fraudulent registration. The use of the ballot locking technology is also seen as a useful innovation. It provides:

a. some protection against ballot modification on the internet hosting server, even from privileged users;

b. increased privacy because of the encryption of the ballot box and the splitting of the decryption over three smart cards;

c. improved secrecy of intermediate results during the polling period;

d. enhanced transparency because of the issue of ballot receipts.

7.1.6 It should be noted that there are a number of residual risks associated with the pilot that were implicitly accepted. They include:

a. risks associated with the untrusted nature of the client PC. These could be subject to malware or virus attacks that could modify the ballot on the client. There is also the potential for 'man in the middle' attacks. Whilst there is no specific evidence of such attacks having occurred during the pilot, this is an area where innovation would be beneficial to improve the security of the system;

b. risks associated with vote buying, selling, trading or vote coercion;

c. risks of wide scale denial of service attacks against the system. There was no evidence of this occurring during the election;

d. risks associated with modification of the voting collection software, which have been mitigated in part by the technical, personnel, physical and procedural measures adopted in the pilot;

e. risks associated with privileged user attack against the counting software, which have been mitigated in part by the technical, personnel, physical and procedural measures adopted in the pilot;

f. risks associated with poor implementation of the voting and counting software. It is recommended that an accreditation scheme be established to mitigate this risk;

g. risks associated with poor configuration and quality management. These risks are avoidable and it should not have been necessary to accept them.

7.2 Evidence of fraud

7.2.1 The Commission has not been made aware of any allegations of fraud or malpractice arising from the pilot scheme at this election. At present, therefore, there is no substantiated evidence to suggest that the procedures provided for by the scheme led to any increase in electoral offences, or in any other malpractice in connection with elections. It is noted that the period in which a prosecution can be launched is one year and so such evidence may still come to light.

8 Cost

8.1 The cost of the pilot is summarised in Table 1. It is noted that these costs are currently being finalised and further minor changes may occur.

Category	Cost (£)	Description
Supplier costs	524,375.00	Provision of staffing (including project mgt.), internet voting solution and call centre set up.
Development expenses	22,000.00	Provision of staffing, technical support and equipment to ensure compatibility with existing systems, manual registration, printing, testing and acceptance.
Operating equipment and call centre	9,500.00	Provision of laptops and staffing costs for voter management and results generation.
Printing of registration forms	5,500.00	Provision of registration forms through third party supplier
Delivery of registration information and voter credentials	17,400.00	Delivery and postage costs of letters/forms and information to electors
Communication plan costs	6,000.00	Costs of delivering the communication plan including posters, banners, on line information, advertisements and giveaways

Table 1 – Pilot costs

8.2 The total cost of the pilot per registered elector is approximately £9.60. The cost per elector that registered to use the service is approximately £87.46. The cost per elector who actually voted is £27.26. The cost per elector that voted using the internet channel is £152.80. It is noted that these costs are significantly higher than more traditional voting methods.

8.3 The breakdown of the Supplier prices is provided in Table 2. It should be noted that these prices are still under discussion and further changes may therefore occur.

Item	Cost (£)
Project Management	45,770
Project support	20,895
Technical Support	25,095
Development Support	25,095
Training Support	4,775

Item	Cost (£)
Quality management	5,970
Call centre costs	4,000
Development and software costs	229,220
Hosting	26,000
Personalisation of the voter interface	7,960
Computer hire	6,000
Credential generation	15,920
Production of the on-line register	7,960
Holding a pre-election trial	5,975
Penetration testing	7,170
Load testing	7,170
Provision of a 24/7 help desk	11,950
System monitoring and reporting	11,950
Audit	22,000
Results and statistics generation	33,500
Total	**524,375**

Table 2 – Supplier price breakdown

8.4 The Technical Evaluator for this pilot was not able to reconcile some of these price items to the prices provided in the initial quotation provided by the supplier. The Evaluator was unable to reconcile the prices to the framework costs. The Evaluator for this pilot was also not in a position to confirm that the items that were common between the South Bucks pilot and the Council's pilot (e.g. penetration testing) had not been charged for twice and the anticipated savings obtained by the sharing of the Internet Voting service between the two pilots had been achieved. It is recommended that a detailed reconciliation be performed by the Council and by MoJ to confirm that final prices are consistent with the contract.

8.5 It is noted that good commercial practice requires that the impact of any significant changes to contract requirements once a contract has been let, should be subject to an impact assessment (including cost and timescale implications) and agreement reached between the supplier and customer on the impact prior to the work being performed. Without this discipline it is difficult to ensure value for money is delivered. It is noted that the tight timescales of the project may have the prevented this process being followed.

8.6 It is noted that the current costs are high and that the supplier in producing their cost model has had to make a series of assumptions to derive its prices (e.g. the number of the potential electorate that will vote using a particular channel for a particular election). It is essential that the MoJ has a good understanding of the supplier cost base and the assumptions that have been made. It is only with this understanding that the MoJ will be able to assess whether the appropriate risks have been transferred to the supplier, whether there is value in the MoJ/LA holding some of these risks and whether the significant price reductions required for delivery enable the cost of Internet voting to be comparable to traditional voting. It is recommend that the MoJ develops and documents a strategy for ensuring the costs of internet voting can be reduced to the required levels and that future pilots should contribute to the delivery of these price reductions.

9 Conclusions

9.1 Introduction

9.1.1 Paragraph 2.3 defined 8 criteria as the basis of the technical evaluation, namely

a. assessment of the degree to which the suppliers have met the requirements of the pilot;

b. analysis of how effective the system was in practice, including accuracy, reliability, robustness, security and functionality aspects;

c. assessment of the risks to the effectiveness of the system;

d. analysis of the adequacy of the development lifecycle, covering project management, risk management, requirements, design, implementation, deployment and testing;

e. analysis of the testing process including accuracy, reliability, robustness, security and performance tests;

f. analysis of the effectiveness of the Quality Assurance (QA) processes performed, together with analysis of the actions taken by suppliers as a result of the QA process commissioned by the Ministry of Justice (MoJ);

g. assessment of any other technical issues that may have affected the success of the local election;

h. assessment of the extent to which the desired technical learning outcomes of the pilot were met and whether any other learning points were developed during the pilot.

9.2 Requirements

9.2.1 The internet voting channel was available to voters as advertised, and was used to cast votes by approximately 3,827 electors. The pilot functionality provided electors with a simple method of casting their votes at their own convenience. It provided them with a receipt confirming that their vote had been recorded by the e-ballot box and enabling them to later confirm that it had been counted when the ballot box was opened.

9.2.2 The supplier met the high level requirements of the pilot. At a detailed level it is not possible to confirm that all the requirements of the pilot were achieved by the supplier. This is because of the lack of detailed documentation and because detailed acceptance of the supplier's solution against all the requirements in the framework contract and pilot SoR was not performed.

9.3 System effectiveness

9.3.1 The system was used successfully by 3,827 electors. No major issues associated with the effectiveness of the system were reported to the Evaluator. It is noted that of the 6,686 people who registered for e-voting only 4,157 (about 62%) attempted to vote and only 57% of the pre-registered voters eventually cast their ballot. The reason for the low percentage of actual voters is not known. It is also noted that:

a. a significant number of users had to contact the call centre because they forgot their username;

b. of those who attempted to vote using the internet channel 3827 (92%) successfully cast their vote. 15 potential voters successfully authenticated themselves to the system but did not cast a vote. 315 potential voters (8%) abandoned their voting attempts completely. Some of these potential voters may not have been legitimate voters who were testing the system. Anecdotal information suggested that some of the users, having initially failed to vote, could not be bothered to contact the call centre.

9.3.2 No significant reliability or robustness issues have been identified with the vote casting system. Issues occurred with the vote tallying system that resulted in approximately ½ hours delay to the count. This issue is directly related to the comprehensiveness of the testing performed prior to the election and was avoidable.

9.3.3 The Evaluator has not been made aware of any allegations of fraud or malpractice arising from the pilot scheme at this election. Nevertheless a number of security concerns were identified as part of the evaluation process, including:

a. the lack of key project documentation;

b. the absence of systematic and rigorous approach to security assessment;

c. the lack of clarity of what the residual security risks that were being accepted and the explicit sign off that these risks were acceptable;

d. the limited nature of the independent security penetration testing performed;

e. the lack of time available to address the security risks identified by the tests performed and independent confirmation that the required remedial work had been correctly performed.

9.4 Risks

9.4.1 The most significant risk to the effectiveness of the system arose from the short timescale available for the design, development and implementation. The supplier indicated that a realistic timescale for the pilot was 6 months. The supplier was required to complete the work in less than 3 months. Insufficient time was allowed for project documentation to be produced and reviewed, the system to be thoroughly tested, remedial work to be performed and required regression testing to be completed.

9.4.2 While no unexpected security risks to the system were identified by the Evaluator, the lack of a systematic security risk assessment undermined overall confidence in the security of the system. Residual risks that the Returning Officer was required to accept were not explicitly identified and agreed. An adequate Risk Management and Accreditation Document Set was not produced.

9.5 Development lifecycle

9.5.1 A number of shortfalls in the development lifecycle have been identified. These include:

a. poor procurement practise;

b. adequate project documentation was not maintained;

c. quality, testing and acceptance procedures were not adequate.

9.5.2 There are significant opportunities for improvement and these are summarised below.

9.6 Testing

9.6.1 Evidence of testing throughout the development lifecycle was not provided. The approach to testing was not comprehensive. Insufficient time was allowed for testing to be performed. Insufficient time was allowed for required remedial work.

9.6.2 The independent penetration testing was limited to black box testing. This was performed in parallel with the suppliers testing. Both the Supplier's testing and the independent testing identified a number of issues that needed to be resolved. There was no independent validation that the required remedial work had been performed.

9.6.3 It is recommended that a full Health Check including both internal and external white box penetration testing by an independent CESG Check approved supplier (or CESG) should be performed for all internet voting pilots. It is recommended that this be performed after the Supplier has performed their own testing and addressed any issues that this testing identified.

9.7 Quality assurance

9.7.1 The quality assurance activities performed by the supplier were not adequate. The issues identified with the quality assurance activities identified are typical of those associated with a project run to very tight timescales.

9.7.2 The independent quality assurance activity performed by the MoJ had a low level of resource associated with it, was focused on the security aspects of the system and was performed just prior to the election starting. A more comprehensive approach to Quality Assurance should be adopted. As recommended in previous Commission reports[8], the independent quality assurance / technical assurance activities should be performed throughout the pilot project and should not delayed to two days before the election is due to commence. This would enable problems to be identified much earlier and appropriate remedial action taken.

9.8 Other issues

9.8.1 While not directly affecting the success of the local election it is noted that, due to the short timescales associated with the pilot implementation, a tight approach to contract management was not adopted.

9.9 Learning points

9.9.1 A significant number of lessons can be learnt from this pilot. These include the need to:

a. provide overall strategic direction to the electoral modernisation programme, ensure lessons highlighted in previous evaluations are learnt, that the strategic direction is communicated to the organisations involved in the piloting and that these organisations can take a longer term view during the piloting programme;

b. ensure that the timescales associated with a piloting exercise are adequate without the need for suppliers to 'cut corners' and with time for full quality assurance and for testing

[8] "The shape of elections to come – a strategic evaluation of the 2003 electoral pilot schemes", The Electoral Commission, 31 July 2003.

activities to be performed and any subsequent required remedial work to be undertaken prior to the election starting;

c. ensure adequate documentation is produced during a pilot and that this documentation is available at an early enough stage for any deficiencies identified as part of review activities to be addressed;

d. ensure that a systematic and comprehensive risk assessment is performed as part of the pilot and that the Returning Officer is made aware of the residual risks he is accepting and explicitly signs to confirm that he is prepared to accept them;

e. ensure that a comprehensive and systematic approach to acceptance testing is put in place. Verification and validation activities should occur throughout the pilot and should not be limited to acceptance testing of the final system a few days before the election;

f. ensure that all involved understand their responsibilities, including their contractual obligations;

g. ensure that independent quality assurance activities are undertaken throughout the pilot activity, not just at the end of the pilot and that sufficient time is allowed for remedial action to be taken. This includes performing adequate quality assurance of potential suppliers as part of the bidding process;

h. ensure that full penetration testing is performed.

9.9.2 It is recommended that quality assurance activities that can be performed prior to a pilot are implemented. There would be significant value in introducing an accreditation scheme for e-voting systems to provide greater confidence in their correct implementation.

9.9.3 It is also recommended that the current procurement approach is reviewed to determine if there is a way in which better value for money can be achieved and that full benefit of the investment made in the development and integration activities is achieved.