SOLGM
NEW ZEALAND SOCIETY OF
LOCAL GOVERNMENT MANAGERS

PART 15
VOTE PROCESSING AND COUNTING

CODE OF GOOD PRACTICE
FOR THE MANAGEMENT OF LOCAL AUTHORITY ELECTIONS AND POLLS 2013

OBJECTIVE OF PART

All electoral officers are familiar with the statutory requirements and recommended procedural practices relating to the handling of voting documents once received from voters.

Being familiar with these requirements and practices will assist achievement of the *Local Electoral Act* principle of public confidence in and understanding of electoral processes.

KEY MESSAGES

Electoral officers:

- need to have good plans in place, covering roll scrutiny and the processing and counting of votes, so as to provide timely and accurate election and poll results
- need to have good plans in place to provide 'end-to-end' assurance for the handling of voting documents from the time they are received from voters to the declaration of results including good security arrangements
- need to be familiar with good practice requirements for managing electronic information systems
- need to have good risk management strategies in place.

CONTENTS

INTRODUCTION

15.1 One of the principles of the *Local Electoral Act 2001 (LEA)* is *"public confidence in, and public understanding of, local electoral processes through … (among other things) procedures that produce certainty in electoral outcomes"*. Critical to the achievement of this principle are the procedures used by the electoral officer once voting documents have been received from voters.

15.2 The procedures used by the electoral officer through this phase of an election or poll relate to four groups of activities:

- scrutiny of the roll
- processing of voting documents
- vote counting
- reporting of election or poll results.

15.3 A number of these tasks rely heavily on electronic technology. As a result, electronic information systems are a critical component of vote processing and counting activities. The introduction of the single transferable vote (STV) electoral system has increased this reliance and emphasises the importance of technological tools in conducting local elections and polls.

15.4 As part of the development of recommended good practice for vote processing and counting activities set out in this Part of the Code, the SOLGM Electoral Working Party has also developed detailed guidance on: determining informal and valid voting documents; the management of electronic information; the STV counting program (STV calculator); and "end-to-end" assurance around the receipt, processing and counting of voting documents. This guidance is set out in appendices.

15.5 This Part of the Code sets out the requirements of the *LEA* and the *Local Electoral Regulations 2001 (LER)* relating to the receipt and processing of voting documents and the counting of votes/preferences, and addresses the following issues including recommended good practices:

(a) roll scrutiny
(b) early processing of votes
(c) Justices of the Peace
(d) vote counting
(e) counting of STV votes
(f) electronic vote processing and counting systems
(g) security of premises and systems
(h) risk management
(i) offences.

15.6 Part 16 covers the reporting of election results.

LEGISLATION

15.7 The key legislative provisions relating to vote processing and counting are:

Local Electoral Act 2001

Section 4	*Principles*
Section 5	*Interpretation*
Section 19AA	*Duties of programmers*
Section 19AB	*Duties of certifiers*
Section 65	*Further notice of election or poll to electors*
Section 73	*Adjournment of election or poll*
Section 74	*Electoral officer to maintain security and secrecy at election or poll*
Section 78	*Voting*
Section 80	*Processing before close of voting*
Section 81	*Scrutineers' presence at processing prohibited before close of voting*
Section 82	*Justices of the Peace to observe processing before close of voting*
Section 83	*Scrutiny of roll*
Section 84	*Counting of votes*
Section 129	*Infringement of secrecy*
Section 130	*Disclosing voting or state of election or poll*

Local Electoral Regulations 2001

Postal voting and FPP (STV):

Regulation 54 (99)	*Voting documents received after close of voting must be marked*
Regulation 55 (100)	*Dealing with returned envelopes*
Regulation 56 (101)	*Processing voting documents during voting period*
Regulation 57 (102)	*Processing voting documents after voting period*
Regulation 58 (103)	*Counting votes*
Regulation 59 (104)	*Checking systems*
Regulation 60 (104A)	*Performance standard for checking systems*
Regulation 61 (105)	*Other disallowed votes*
Regulation 67 (112)	*Security of voting documents*
Regulation 68 (113)	*Electoral officer may announce number of voting documents sent and returned*

(NOTE: Similar regulations also apply for booth voting using FPP and STV and must be followed if this voting method is adopted.)

Regulation 90B	*Multiple elections with common candidates*
Regulation 138	*Eligibility of Justices to observe processing of voting documents*
Schedule 1A	*New Zealand method of counting single transferable votes*

REQUIREMENTS AND RECOMMENDED PRACTICES

(a) Roll scrutiny

15.8 The purpose of the roll scrutiny is to validate, from unopened envelopes, the votes cast in any election or poll. *Section 83(1) LEA* requires the electoral officer to record the name of all electors who appear to have voted and to be satisfied that each elector has voted only once. Where more than one vote is recorded against an elector then all votes cast in that elector's name must be disallowed.

15.9 An added responsibility for the electoral officer is that notwithstanding *section 83(1),* if the electoral officer is satisfied that the elector cast only one vote and was not involved in the other votes cast in the elector's name then the vote cast by the elector must be allowed and the other vote(s) disallowed.

15.10 For postal voting the scrutiny may begin at any time before the close of voting. However, electoral officers must decide dates and times that the scrutiny will be undertaken and notify candidates and their nominated scrutineers. If early processing has been adopted then the scrutiny must be carried out before the votes are opened and processed.

15.11 The roll or rolls used for the scrutiny must be kept until the next triennial general election of members and during that period must be available for public inspection, without fee, during the hours the offices of the local authority are open to the public *(Regulations 69 and 86)*.

1 Recommended good practice on roll scrutiny is that electoral officers:

(i) plan in advance to ensure that the roll scrutiny is commenced as early as possible to avoid any delay in declaring the preliminary result of the election or poll

(ii) ensure that all candidates and scrutineers are advised, in advance, of the roll scrutiny arrangements

(iii) ensure that the roll scrutiny is included in security arrangements relating to the election or poll.

(b) Early processing of votes

15.12 *Section 80 LEA* authorises electoral officers, at their discretion, to decide to process voting documents during the voting period in respect of an election or poll. It is strongly recommended that electoral officers do process voting documents during the voting process as this is now accepted as good practice given it allows electoral officers to cost-effectively manage their resources in this period and it removes the pressure, and resulting likelihood of errors, that arise if processing is delayed until the close of voting.

15.13 If early processing of voting documents is to take place, *section 80* requires the electoral officer to process the voting documents in the prescribed manner. It also sets out requirements where early processing has commenced but is not complete at the close of voting. *Regulations 54 to 57* relating to first past the post (FPP), and *regulations 99 to 102* relating to STV, prescribe the requirements for receipt and processing of voting documents during and after the voting period. These requirements include that the scrutiny of the roll must be completed before processing commences.

2 Recommended good practice on early processing of votes is that electoral officers familiarise themselves with and take full advantage of the early processing requirements of the *LEA.*

(c) Justices of the Peace (JPs)

15.14 *Section 82* requires the electoral officer to appoint at least one JP to be present and observe all steps in the processing of voting documents under *section 80*. *Regulation 138* sets eligibility criteria for JPs. All JPs are required to provide the electoral officer with a certificate stating whether or not the JP is satisfied, that *section 80* and the regulations governing early processing of voting documents, were complied with. If not satisfied, the JP must attach a report to the certificate setting out any way in which the section or regulations were not complied with.

15.15 It is important to note that while a JP must be present during early processing of votes, the presence of scrutineers during early processing of votes before the close of voting is prohibited.

15.16 When considering the introduction of early processing, the Internal Affairs and Local Government Select Committee recommended, in the report on its 'Inquiry into the Early Processing of Voting Papers at Local Authority Elections', that SOLGM and the Royal Federation of New Zealand Justices Association develop training for JPs.

15.17 The SOLGM Electoral Working Party agrees that training for JPs, involved in the processing of voting documents before close of voting, is beneficial. However, there will be differences between local authorities in how they conduct early processing of voting documents (period of time, computer systems, etc). Therefore it is considered that electoral officers should develop and tailor their own briefing/training sessions for JPs involved in observing the processing of voting documents before the close of voting.

3 Recommended good practice on Justices of the Peace (JPs) is that electoral officers:

(i) provide a brief on what the role and requirements of JPs are in relation to early processing of voting documents to the local branch of the Royal Federation of New Zealand Justices Associations and obtain a list of recommended JPs

(ii) develop and hold training sessions for JPs covering the processing systems and security issues etc relating to the processing of voting documents before the close of voting

(iii) ensure that at least one appointed JP is present when any early processing of voting documents is undertaken

(iv) ensure that if a JP is allocated with a password to the electoral software, that he/she is able to be present on polling day after the close of polling to unlock the security system on the electoral software

(v) ensure that JPs are not involved in other work or duties associated with the election or poll outside their role in relation to the processing of voting documents before close of voting.

(d) Vote counting

15.18 How the votes are counted will depend upon the electoral system (FPP or STV) and voting method (postal or booth voting) used in each area. In addition, manual or electronic counting systems may be used. Requirements are set out in *section 84* and in *regulation 58* in respect of FPP using postal voting and *regulation 103* in respect of STV using postal voting.

15.19 For postal voting, where early processing has been adopted, the electoral officer may process but not count voting documents during the voting period. Counting, whether early processing has been adopted or not, may only take place after the close of voting. It must commence as soon as practicable after the close of voting and after processing has been completed.

15.20 A key element of vote counting is the determining of valid voting documents. This differs depending on whether the FPP or the STV electoral system is used. *Regulation 48* defines "valid" in respect of FPP voting documents and *regulation 91* in respect of STV voting documents. In short, valid voting documents are voting documents that are not blank or informal (as defined in *regulations 48* and *91*) or disallowed under *regulations 61(2)* or *80(2)* for FPP voting documents or *regulations 105(2)* or *125(2)* for STV voting documents. Electoral officers responsible for counting votes need to be familiar with these definitions and more detailed guidance developed by the SOLGM Electoral Working Party is provided in *Appendix A*.

15.21 The electoral officer must apply a checking system to the processing and counting of votes. The requirements relating to checking systems are set out in *regulations 59 and 104* in relation to FPP and STV respectively. *Regulations 60 and 104A* set out the performance standards for checking systems. The performance standards state that:

(1) The checking system must ensure that the results of the counting are at least as accurate as those that would be produced by:

(a) carrying out the following operations manually

(i) rejecting blank voting documents and informal voting documents

(ii) counting/recording votes from valid voting documents

(b) repeating the operations in paragraph (a)

(c) resolving any discrepancies.

(2) In determining whether or not the performance standard in subclause (1) is met, it is sufficient to make reasonable inferences about the errors that are likely to be generated by the operations specified in subclause (1)(a).

15.22 *Regulation 90B* provides that in the case of multiple elections with common candidates (e.g. common candidates for mayor and councillor or for councillor and community board member), the electoral officer must count the votes for these elections in this order: first the mayor, then council, then community board.

4 Recommended good practice on vote counting is that electoral officers:

(i) develop and test before the election, a process for counting votes that suits the electoral system and voting method to be used

(ii) are familiar with definitions of valid, blank, informal and disallowed voting documents in respect of FPP and STV voting documents

(iii) adopt a checking system that ensures that the performance standards required under regulation are achieved.

(e) Counting of STV votes

15.23 The *LER* defines STV as the electoral system (described in *section 5B LEA)* using the New Zealand method of counting single transferable votes. This method of counting votes is set out in *Schedule 1A LER*.

15.24 The New Zealand method of counting single transferable votes, given its nature, requires the use of computers. This applies in the case of all DHB elections, for which STV is mandatory, and those local authorities that have resolved to use STV or are required to use STV as the result of a local poll.

15.25 *Section 19AA* requires every person responsible for the design of a counting program intended to implement the New Zealand method of counting single transferable votes, to take all reasonable steps to ensure that the program produces outcomes consistent with the process specified in *Schedule 1A LER*.

15.26 *Section 19AB* states that a counting program may not be used at an election or poll under the *LEA* for the purpose of implementing the New Zealand method of counting single transferable votes unless it has been certified for the purpose by the Secretary for Local Government.

15.27 The Department of Internal Affairs was responsible for the development of a counting program designed to implement the New Zealand method of counting single transferable votes. This program (the STV calculator) has been certified for use in STV elections as required by *section 19AB*. The Department provides the STV calculator (and a backup calculator) free of charge on a licence basis to local authority electoral officers undertaking the counting of STV votes using the New Zealand method of counting single transferable votes. It is not mandatory to use the STV calculator however it is recommended.

5 Recommended good practice on counting of STV votes is that electoral officers responsible for counting STV votes use the STV calculator supplied by the Department of Internal Affairs for this purpose.

(g) Electronic vote processing and counting systems

15.28 Because of the importance of information technology systems in the election process, separate handbooks have been prepared entitled *Managing the Electronic Information* and *The STV Calculators – Tips and Tricks*. These are included as *Appendices B* and *C* to this Part of the Code.

15.29 The handbook *Managing the Electronic Information* covers a wide range of IT issues including:

- physical security
- network security
- data security
- staff organisation
- communications security
- data interchange
- computer operating systems
- system performance factors
- application software
- results reporting
- STV calculators
- scanners
- electronic rolls
- voting document processing procedures
- audit trails.

15.30 The handbook *The STV Calculators – Tips and Tricks* has sections relating to:

- preparing the main calculator
- the graphical user interface
- resolving problems
- the "backup" calculator.

6 Recommended good practice on electronic processing and counting systems is that electoral officers be familiar with the contents of the two handbooks *Managing the Electronic Information* and *The STV Calculators – Tips and Tricks* and use these handbooks (see *Appendices B* and *C*), as appropriate, when conducting elections and polls.

(f) Security of premises and systems

15.31 There may be public concern about vote secrecy and the security of voting documents being processed before the close of voting. *Section 74* and *regulations 67* and *112* charge the electoral officer with responsibility for the security of the voting documents at all times and their secrecy. Therefore, in terms of premises and electronic vote processing systems, there are several practices/procedures which should be implemented to alleviate secrecy and security concerns surrounding voting documents. Good practice recommendations relating to security for electronic vote processing and counting systems are included in *Appendix B – Managing the Electronic Information*.

15.32 Access to the premises where voting documents are being processed must be carefully managed and restricted to the electoral officer, electoral staff (i.e. not other local authority staff) and Justices of the Peace. If any other persons request access or are to be invited, such as Department of Internal Affairs officials or other visiting electoral officials, recommended good practice is for these people to be required to sign an appropriate declaration form before access is granted.

7 Recommended good practice on security of premises and systems is that electoral officers:

(i) use premises that are:

- lockable and secure (if necessary, change the locks for the polling period)
- private (processing cannot be viewed through windows, open doors etc)
- contain a fireproof and lockable room to store all ballot boxes and voting documents

(ii) use separate rooms for the scrutiny of the roll and any early processing of voting documents if the same premises are used for these functions. (If the same room is to be used, it is important to ensure that the scrutiny procedures are fully completed, envelopes locked away and scrutineers have left the premises before processing commences)

(iii) ensure only the electoral officers and electoral staff that have signed a declaration under *section 14(2)*, have access to any room(s) where processing is to occur and appropriate signage is provided outside the room prohibiting entry

(iv) require any visitors inspecting vote processing to also sign a declaration

(v) adopt the recommended physical security practices set out in *Appendix B – Managing the Electronic Information*.

(h) Risk management

15.33 Electoral officers can expect close scrutiny from the media, politicians and their local community in the running of local elections and the timely announcement of results. Good planning and management are essential to meet these expectations and planning should include risk management. While this applies for all election tasks, a particular focus should be on activities and issues relating to processing voting documents to allow the timely release of accurate election results.

15.34 To assist electoral officers in this area the SOLGM Electoral Working Party has developed guidelines for achieving 'end-to-end' assurance on vote processing and counting for local elections and polls. These are attached as *Appendix D*. In these guidelines 'end-to-end' is defined as commencing with the receipt of returned voting documents from voters to the production of election results. The guidelines apply, with any necessary modifications, whether postal or booth voting is used, or whether FPP or STV is being used.

15.35 Electoral officers are encouraged to assess what could go wrong at any election or poll, not just in relation to vote processing and counting, and to plan for contingencies.

15.36 The local environment and the community in which each election or poll is run will vary considerably and so there can be no master contingency plan that suits all circumstances. The way in which the election or poll is being run i.e. by a service provider, in-house, or a combination of service provider/in-house, will also present areas of risk.

15.37 As a starting point the following is a list of risks and possible mitigation steps that electoral officers should consider in the development of an elections and polls risk management strategy:

- software failure – use independently assured 'fit for purpose' software accompanied by adequate documentation, carry out plenty of testing and training, make arrangements for software support
- under resourced – have arrangements that you can quickly put in place if you are, for example, overwhelmed with greater returns of voting documents than predicted
- equipment failure – identify where you could immediately obtain replacement equipment and get support to set up the new equipment
- power failure – have contingencies for an uninterruptible power supply at least for your server and backup generator
- loss of premises – identify alternative premises and have a business continuity plan
- breach of security – identify steps to address breaches of physical and data/ network security
- destruction/loss of voting documents – ensure secure storage to mitigate this risk
- loss of voting documents in transit (e.g. when transferred for processing) – ensure reliable and safe transport arrangements to mitigate this risk
- lack of management controls – identify contingencies to address risks such as inadequate software version control
- postal delivery problems – consider what action you would need to take if parts of a community do not receive voting documents
- subcontractor failing to deliver – ensure due diligence and contingency operations
- natural disasters, major industrial disputes etc – identify possible steps if these are localised events.

15.38 It is noted that *section 73* provides for the electoral officer, in the event of a natural disaster, adverse weather conditions, breakdown of communication or energy services, riot or disorder, or any other event, to adjourn the close of voting for a period of 14 days. This adjournment of the close of voting may continue, if necessary, until the election or poll can be held. This provision relates to situations or events that would, in the view of the electoral officer, deny electors a reasonable opportunity to cast a valid vote i.e. it applies up to the close of voting. While responsibility lies with the electoral officer concerned, he or she needs to be aware that advice and support is available should such a serious situation arise. It is recommended, therefore, that electoral officers seek the advice and assistance of the Chair of the SOLGM Electoral Working Party before taking action under *section 73*.

15.39 New *Section 73* provides for the Governor-General, by Order in Council, to adjourn certain electoral processes at triennial local authority elections when this is considered necessary for ensuring that the adverse effects of an emergency (whether local or national) or other event, do not deny electors a reasonable opportunity to cast a valid vote, nominate a candidate, or accept nomination as a candidate in relation to the election in question. The section provides for an adjournment of the process or processes for a maximum of six weeks. The Order must be made on the recommendation of the Minister of Local Government. It is recommended that electoral officers be familiar with these provisions and if it is considered they are or might be needed, the electoral officer contact the Chair of the SOLGM Electoral Working Party in the first instance as a matter of priority to seek advice and support.

8 Recommended good practice on risk management is that electoral officers:

(i) adopt the good practice steps set out in the 'Vote Processing and Counting Assurance Guidelines' (*Appendix D*)

(ii) assess what could go wrong in other local election or poll operations for which they are responsible and consider how best to mitigate the risks and deal with any resultant emergency.

(iii) familiarise themselves with the provisions of *sections 73* and *73A LEA* and contact the Chair of the SOLGM Electoral Working Party, as a matter of priority, in the event that they are or could be needed in respect of an election or poll.

(i) Offences

15.40 There are offence provisions relating to the infringement of secrecy of voting (*section 129*) and disclosing voting *(section 130)* and electoral officers should be familiar with these.

9 Recommended good practice on offences is that electoral officers ensure that all election officials are aware of actions or inactions when handling voting documents that constitute an offence and the associated penalties.

SOLGM
NEW ZEALAND SOCIETY OF
LOCAL GOVERNMENT MANAGERS

PART 15: APPENDIX A GUIDANCE ON DETERMINING INFORMAL AND VALID VOTING DOCUMENTS

CODE OF GOOD PRACTICE
FOR THE MANAGEMENT OF LOCAL AUTHORITY ELECTIONS AND POLLS 2013

CONTENTS

INTRODUCTION

The following guidelines have been developed by the SOLGM Electoral Working Party to assist electoral officers and their electoral officials determine, on how the voter has completed their voting document, whether the voting document is valid or informal. These guidelines augment the guidance in Part 15: Appendix D – Vote Processing and Counting Assurance. In particular they will be helpful as part of the 'performance standard checking system' required under *clauses 79(b)(FPP)* and *104A(STV)* of the *Local Electoral Regulations 2001*.

LEGISLATION

Key provisions relating to informal voting documents are the following definitions in the *Local Electoral Regulations 2001*.

(a) **FPP**

Clause 48(1) defines 'informal voting document' as a voting document –

'…

(a) that the electoral officer has reasonable cause to believe was not issued to an elector by the electoral officer or other electoral official; or

(b) on which the number of candidates for whom the voter has voted exceeds the number of candidates to be elected; or

(c) is not a blank voting document and does not clearly indicate the candidate or candidates for whom the voter desired to vote …'

(For the purposes of this guidance, paragraphs (b) and (c) are the applicable provisions.)

(b) **STV**

Clause 91(1) defines 'informal voting document' as a voting document that

'…

(a) the electoral officer has reasonable cause to believe was not issued to an elector by the electoral officer or other electoral official; or

(b) is not a blank voting document and does not clearly indicate the voter's unique first preference. …'

(For the purposes of this guidance, paragraph (b) is the applicable provision.)

In addition to the above informal voting document definitions, a relevant legal opinion from Simpson Grierson is appended.

EXAMPLES OF VALID AND INFORMAL VOTING DOCUMENTS

The following examples of informal or valid voting documents have been developed taking into account:

(a) the Principles of the *Local Electoral Act* in *section 4*, particularly *subsection (1)(b) – "all qualified persons have a reasonable and equal opportunity to:*
(i) cast an informed vote"

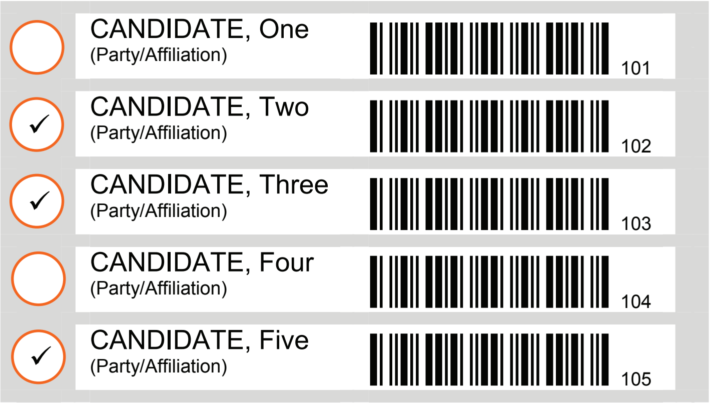
(b) that an informal voting document is one which is not blank but is so marked to:
(i) show the voter has voted for more candidates than allowed; or
(ii) not clearly indicate the candidate or candidates for whom the voter desired to vote; or
(iii) not clearly indicate the voter's unique first preference (in the case of STV).

From this approach there is a wide range of examples of how voters may mark their voting documents by not using the FPP ✓ or the STV 1, 2, 3, etc, preference ranking, but can still complete a valid vote.

It is advised that if you rule voting documents as valid based on the following examples you should ensure that JPs and any scrutineers involved in the vote counting process are aware of the reasons why the voting document is valid.

FPP ELECTIONS

1 FPP – Vote for 3 Candidates

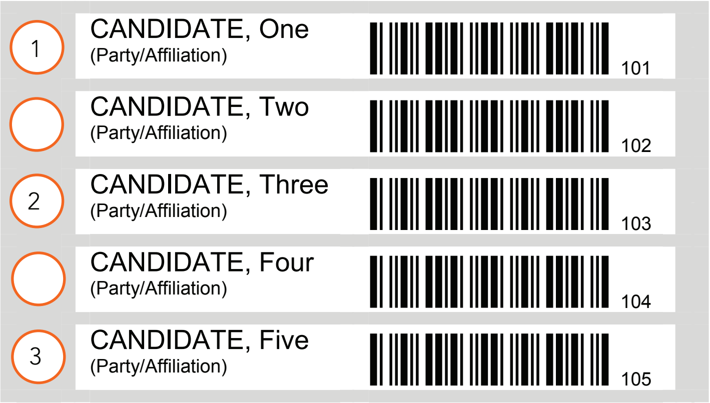


○	CANDIDATE, One (Party/Affiliation)	101
✓	CANDIDATE, Two (Party/Affiliation)	102
✓	CANDIDATE, Three (Party/Affiliation)	103
○	CANDIDATE, Four (Party/Affiliation)	104
✓	CANDIDATE, Five (Party/Affiliation)	105

Allow

Voter has ticked the maximum allowed of three candidates they want to vote for

2 FPP – Vote for 3 Candidates

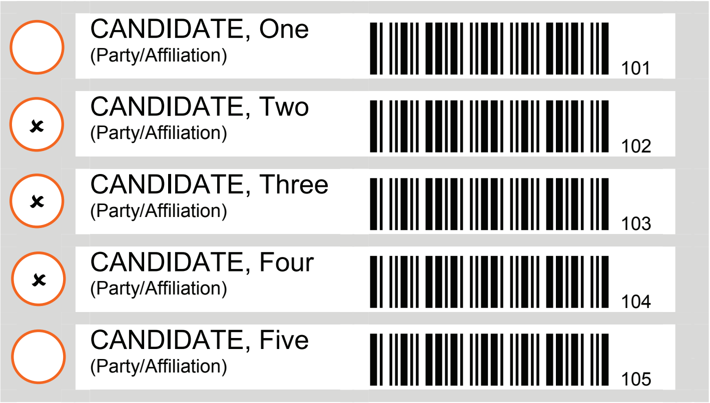


1	CANDIDATE, One (Party/Affiliation)	101
○	CANDIDATE, Two (Party/Affiliation)	102
2	CANDIDATE, Three (Party/Affiliation)	103
○	CANDIDATE, Four (Party/Affiliation)	104
3	CANDIDATE, Five (Party/Affiliation)	105

Allow

Voter has clearly indicated the maximum allowed three candidates they want to vote for

3 FPP – Vote for 3 Candidates

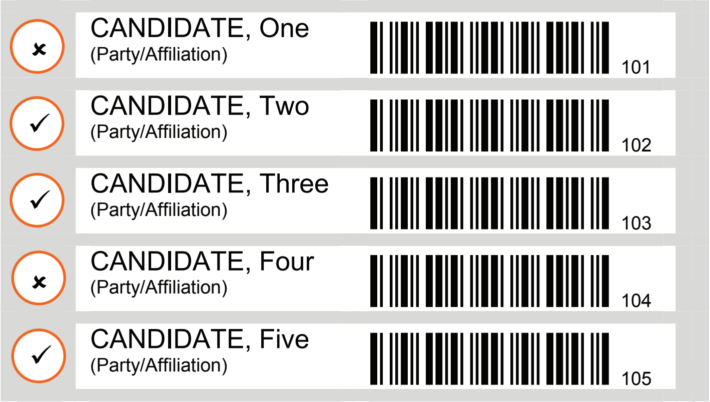


○	CANDIDATE, One (Party/Affiliation)	101
×	CANDIDATE, Two (Party/Affiliation)	102
×	CANDIDATE, Three (Party/Affiliation)	103
×	CANDIDATE, Four (Party/Affiliation)	104
○	CANDIDATE, Five (Party/Affiliation)	105

Allow

Voter has clearly indicated the maximum allowed three candidates they want to vote for

4 FPP – Vote for 3 Candidates

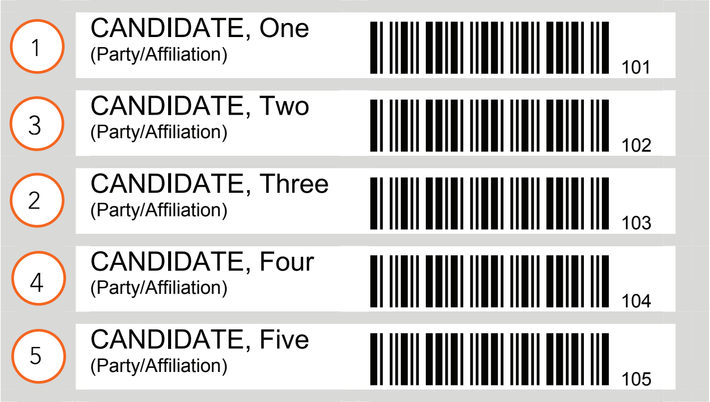


×	CANDIDATE, One (Party/Affiliation)	101
✓	CANDIDATE, Two (Party/Affiliation)	102
✓	CANDIDATE, Three (Party/Affiliation)	103
×	CANDIDATE, Four (Party/Affiliation)	104
✓	CANDIDATE, Five (Party/Affiliation)	105

Allow

Voter has indicated the maximum allowed three candidates they want to vote for and two candidates they do not want to vote for through crosses

5 FPP – Vote for 3 Candidates

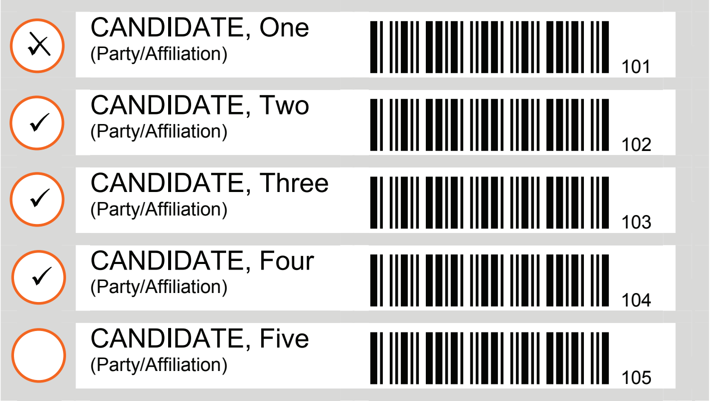


1	CANDIDATE, One (Party/Affiliation)	101
3	CANDIDATE, Two (Party/Affiliation)	102
2	CANDIDATE, Three (Party/Affiliation)	103
4	CANDIDATE, Four (Party/Affiliation)	104
5	CANDIDATE, Five (Party/Affiliation)	105

Disallow as Informal

The voter has voted for more candidates than the maximum allowed and the order of numbering (as for STV) cannot be taken as the voter's preferred three candidates

6 FPP – Vote for 3 Candidates

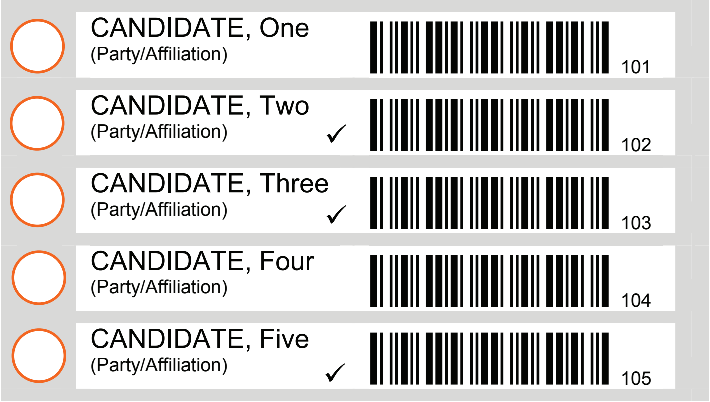


~~✓~~	CANDIDATE, One (Party/Affiliation)	101
✓	CANDIDATE, Two (Party/Affiliation)	102
✓	CANDIDATE, Three (Party/Affiliation)	103
✓	CANDIDATE, Four (Party/Affiliation)	104
○	CANDIDATE, Five (Party/Affiliation)	105

Allow

The voter's intention to vote for the maximum of candidates 2, 3 and 4 is clear. The vote for candidate 1 has been crossed out

7 FPP – Vote for 3 Candidates

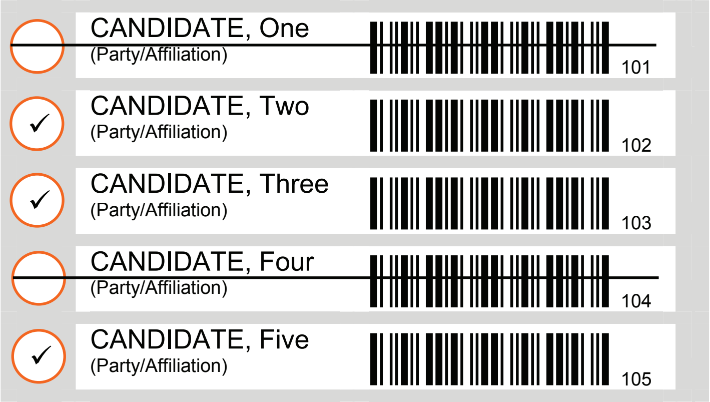


○	CANDIDATE, One (Party/Affiliation)		101
○	CANDIDATE, Two (Party/Affiliation)	✓	102
○	CANDIDATE, Three (Party/Affiliation)	✓	103
○	CANDIDATE, Four (Party/Affiliation)		104
○	CANDIDATE, Five (Party/Affiliation)	✓	105

Allow

Although the voter has not ticked in the 'circle' alongside the candidates 2,3 and 5, their intention to vote for those candidates is clearly indicated and is within the maximum allowed

8 FPP – Vote for 3 Candidates

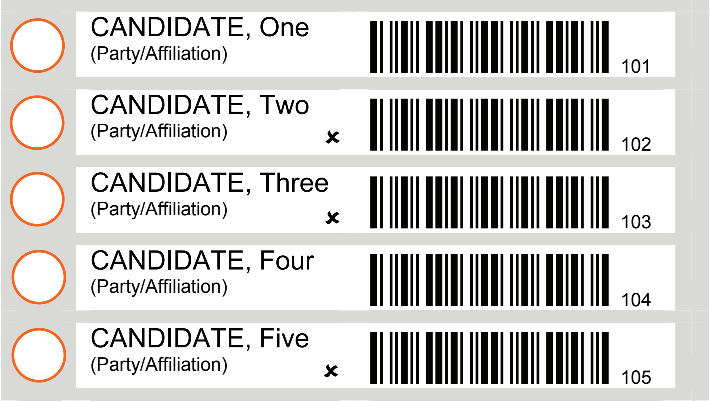


~~○~~	~~CANDIDATE, One~~ ~~(Party/Affiliation)~~	~~101~~
✓	CANDIDATE, Two (Party/Affiliation)	102
✓	CANDIDATE, Three (Party/Affiliation)	103
~~○~~	~~CANDIDATE, Four~~ ~~(Party/Affiliation)~~	~~104~~
✓	CANDIDATE, Five (Party/Affiliation)	105

Allow

The voter has clearly in a positive manner indicated three candidates they want to vote for and two candidates they do not want to vote for

9 FPP – Vote for 3 Candidates

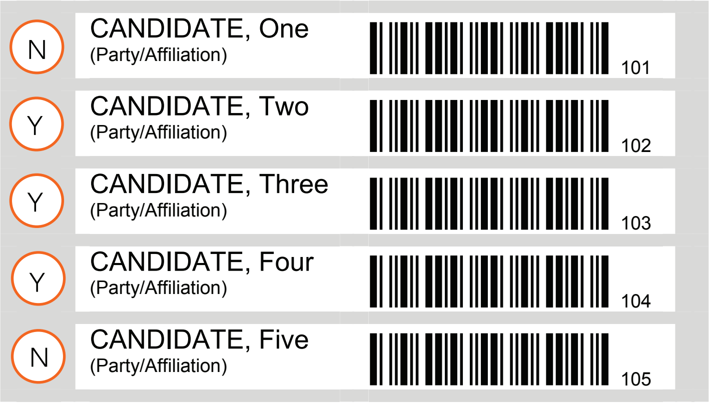


○	CANDIDATE, One (Party/Affiliation)		101
○	CANDIDATE, Two (Party/Affiliation)	✗	102
○	CANDIDATE, Three (Party/Affiliation)	✗	103
○	CANDIDATE, Four (Party/Affiliation)		104
○	CANDIDATE, Five (Party/Affiliation)	✗	105

Allow

Although the voter has not ticked in the 'circle' alongside candidates 2,3 and 5, their intention to vote for those candidates is clearly indicated notwithstanding they have used a cross

10 FPP – Vote for 3 Candidates



N CANDIDATE, One (Party/Affiliation) 101

Y CANDIDATE, Two (Party/Affiliation) 102

Y CANDIDATE, Three (Party/Affiliation) 103

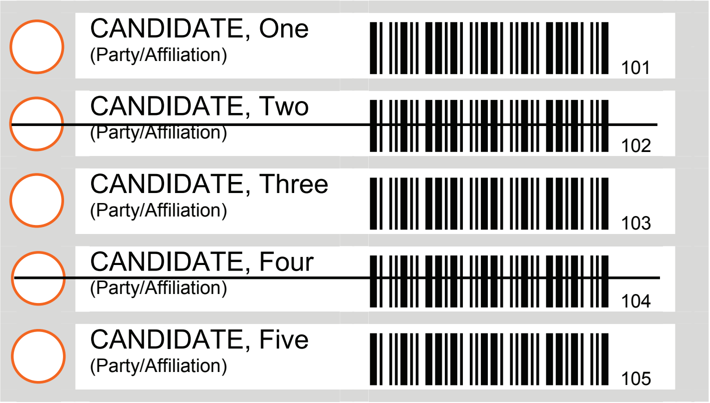
Y CANDIDATE, Four (Party/Affiliation) 104

N CANDIDATE, Five (Party/Affiliation) 105

Allow

The voter has clearly indicated their intention, within the maximum allowed, by assigning 'Y' for 'yes' for candidates 2, 3 and 4 and a 'N' for 'no' for candidates 1 and 5

11 FPP – Vote for 3 Candidates



○ CANDIDATE, One (Party/Affiliation) 101

○ CANDIDATE, Two ~~(Party/Affiliation)~~ 102

○ CANDIDATE, Three (Party/Affiliation) 103

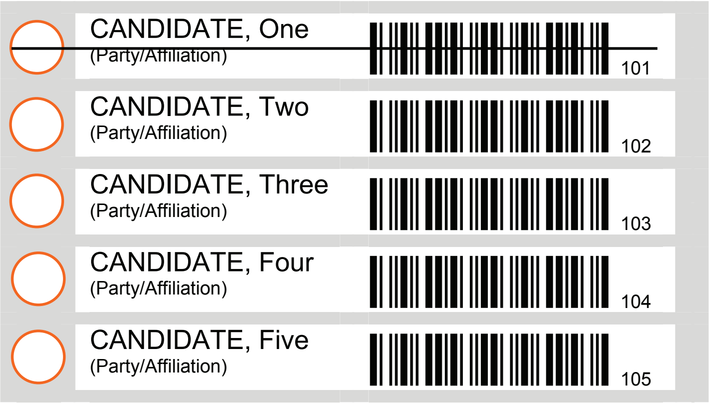
○ CANDIDATE, Four ~~(Party/Affiliation)~~ 104

○ CANDIDATE, Five (Party/Affiliation) 105

Allow

Although the voter has not marked the circles they have clearly indicated their intention, within the maximum allowed, to vote for candidates 1, 3 and 5 by crossing out candidates 2 and 4

12 FPP – Vote for 3 Candidates



○ CANDIDATE, One ~~(Party/Affiliation)~~ 101

○ CANDIDATE, Two (Party/Affiliation) 102

○ CANDIDATE, Three (Party/Affiliation) 103

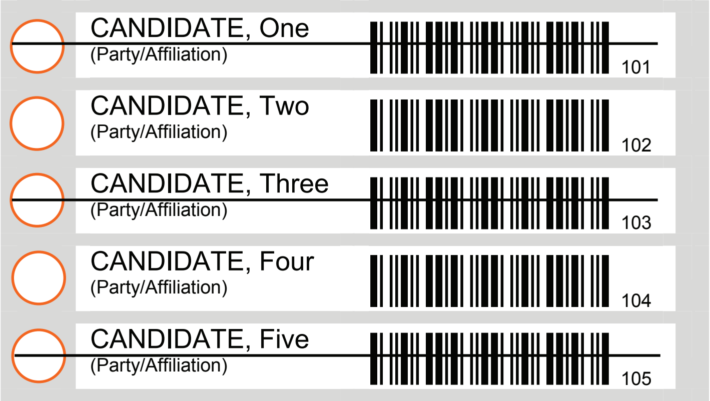
○ CANDIDATE, Four (Party/Affiliation) 104

○ CANDIDATE, Five (Party/Affiliation) 105

Disallow as Informal

The voter has indicated that they did not want to vote for candidate 1 and by inference has indicated they are voting for the other four candidates instead of only a maximum of three candidates allowed

13 FPP – Vote for 3 Candidates



~~○ CANDIDATE, One (Party/Affiliation) 101~~

○ CANDIDATE, Two (Party/Affiliation) 102

~~○ CANDIDATE, Three (Party/Affiliation) 103~~

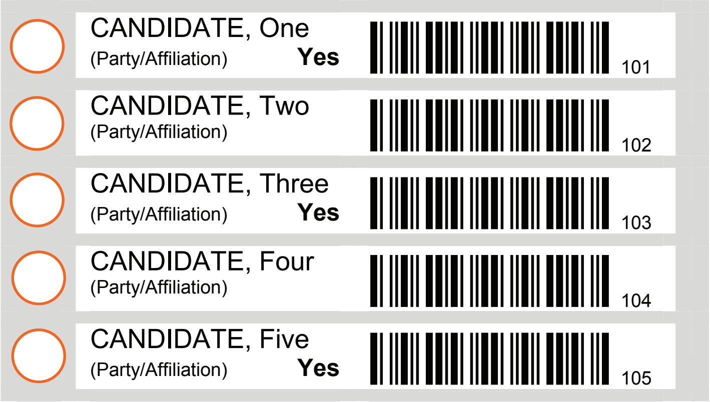
○ CANDIDATE, Four (Party/Affiliation) 104

~~○ CANDIDATE, Five (Party/Affiliation) 105~~

Allow

The voter has clearly indicated intention to vote for candidates 2 and 4 by crossing out candidates 1, 3 and 5. The elector does not have to vote for the maximum of three candidates allowed

14 FPP – Vote for 3 Candidates



○ CANDIDATE, One (Party/Affiliation) Yes 101

○ CANDIDATE, Two (Party/Affiliation) 102

○ CANDIDATE, Three (Party/Affiliation) Yes 103

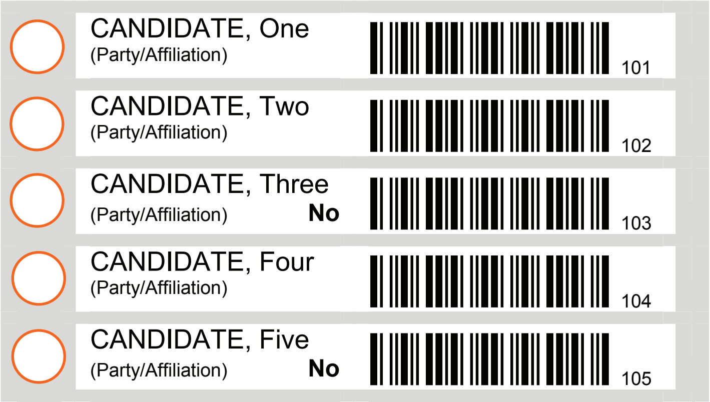
○ CANDIDATE, Four (Party/Affiliation) 104

○ CANDIDATE, Five (Party/Affiliation) Yes 105

Allow

Although the voter has not ticked or otherwise marked the 'circle' alongside candidates 1, 3 and 5, they have indicated clearly their intention to vote for those candidates – the maximum allowed

15 FPP – Vote for 3 Candidates



○ CANDIDATE, One (Party/Affiliation) 101

○ CANDIDATE, Two (Party/Affiliation) 102

○ CANDIDATE, Three (Party/Affiliation) No 103

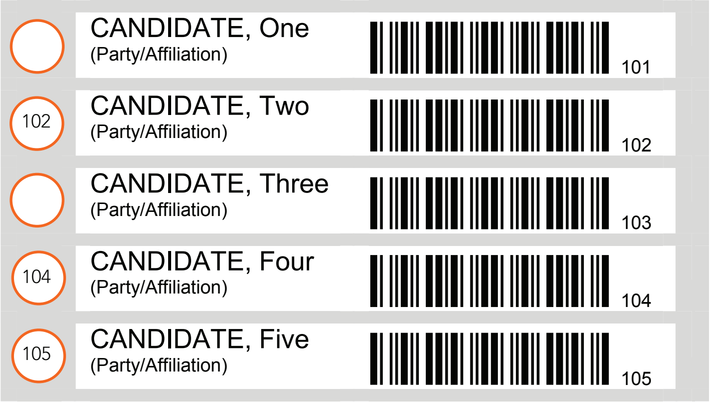
○ CANDIDATE, Four (Party/Affiliation) 104

○ CANDIDATE, Five (Party/Affiliation) No 105

Allow

Although the voter has not ticked or otherwise marked the 'circle' alongside the names of candidates 1, 2 and 4, they have indicated their intention to vote for them, the maximum allowed, by writing 'no' alongside the names of candidates 3 and 5

16 FPP – Vote for 3 Candidates

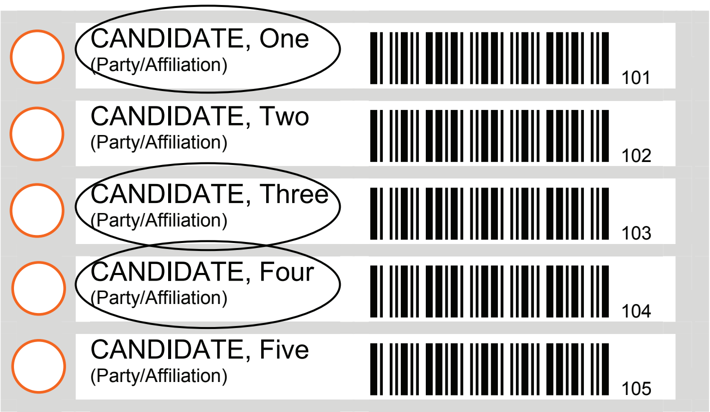


○	CANDIDATE, One (Party/Affiliation)	101
102	CANDIDATE, Two (Party/Affiliation)	102
○	CANDIDATE, Three (Party/Affiliation)	103
104	CANDIDATE, Four (Party/Affiliation)	104
105	CANDIDATE, Five (Party/Affiliation)	105

Allow

The voter has made their intention clear to vote for candidates 2, 4 and 5, the maximum allowed, by writing their candidate readable barcode number in the ‘circle’ alongside their name

17 FPP – Vote for 3 Candidates

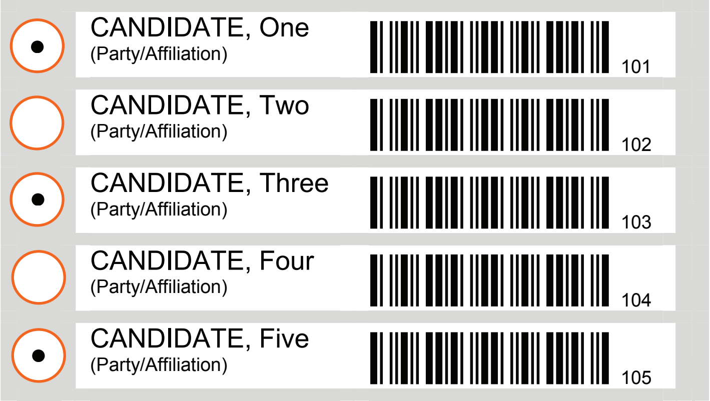


○	[✓ CANDIDATE, One (Party/Affiliation)]	101
○	CANDIDATE, Two (Party/Affiliation)	102
○	[✓ CANDIDATE, Three (Party/Affiliation)]	103
○	[✓ CANDIDATE, Four (Party/Affiliation)]	104
○	CANDIDATE, Five (Party/Affiliation)	105

Allow

Although the voter has not marked the ‘circle’ alongside candidates 1, 3 and 4, their intention to vote for those candidates, the maximum allowed, is clear by circling their names

18 FPP – Vote for 3 Candidates

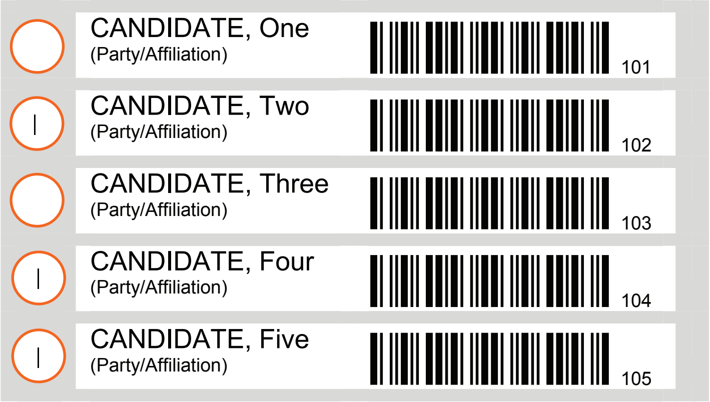


●	CANDIDATE, One (Party/Affiliation)	101
○	CANDIDATE, Two (Party/Affiliation)	102
●	CANDIDATE, Three (Party/Affiliation)	103
○	CANDIDATE, Four (Party/Affiliation)	104
●	CANDIDATE, Five (Party/Affiliation)	105

Allow

The voter has clearly indicated their intention to vote for candidates 1, 3 and 5, the maximum allowed, by marking the circle alongside their name

19 FPP – Vote for 3 Candidates

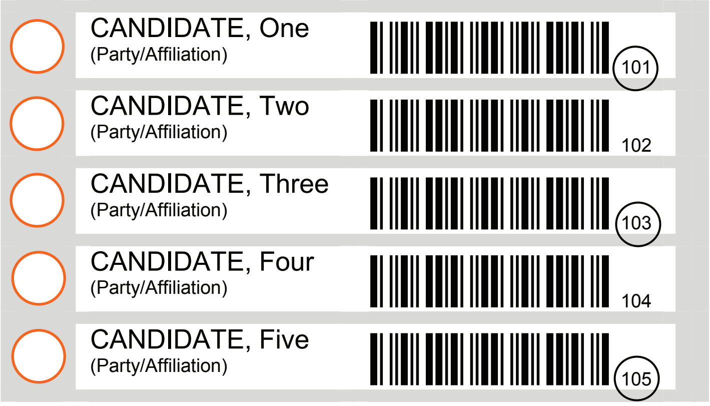


○	CANDIDATE, One (Party/Affiliation)	101
I	CANDIDATE, Two (Party/Affiliation)	102
○	CANDIDATE, Three (Party/Affiliation)	103
I	CANDIDATE, Four (Party/Affiliation)	104
I	CANDIDATE, Five (Party/Affiliation)	105

Allow

As for example 18, the voter has clearly indicated their intention to vote for candidates 2, 4 and 5, the maximum allowed, by marking the 'circle' alongside their name

20 FPP – Vote for 3 Candidates

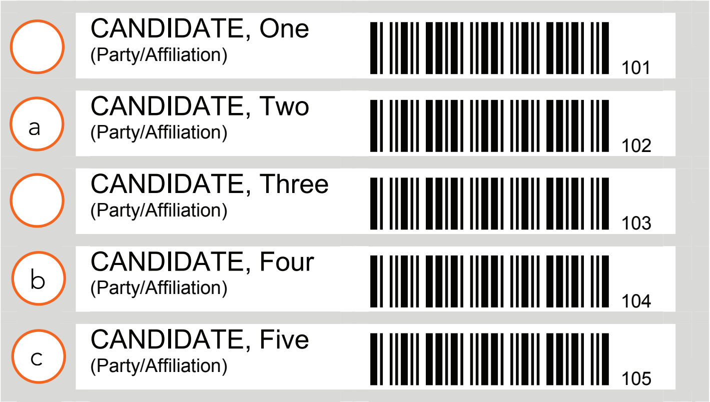


○	CANDIDATE, One (Party/Affiliation)	101
○	CANDIDATE, Two (Party/Affiliation)	102
○	CANDIDATE, Three (Party/Affiliation)	103
○	CANDIDATE, Four (Party/Affiliation)	104
○	CANDIDATE, Five (Party/Affiliation)	105

Allow

The voter has made their intention clear to vote for candidates 1, 3 and 5, the maximum allowed, by circling their candidate barcode readable number

21 FPP – Vote for 3 Candidates



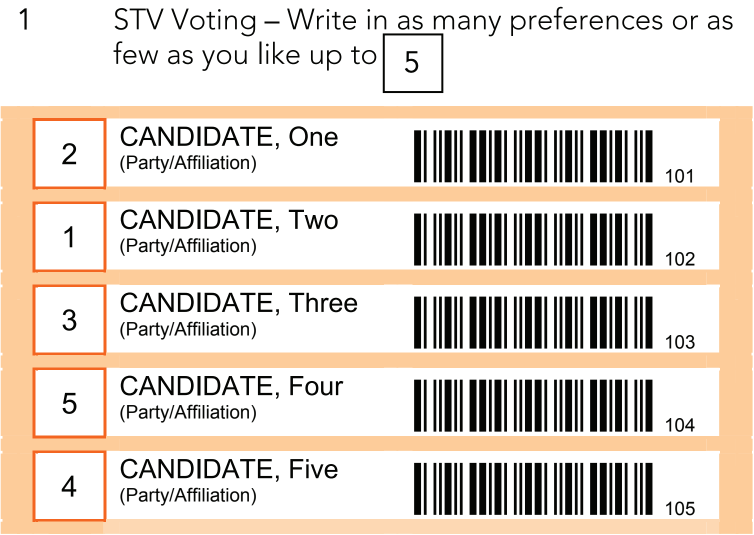
○	CANDIDATE, One (Party/Affiliation)	101
a	CANDIDATE, Two (Party/Affiliation)	102
○	CANDIDATE, Three (Party/Affiliation)	103
b	CANDIDATE, Four (Party/Affiliation)	104
c	CANDIDATE, Five (Party/Affiliation)	105

Allow

The voter has made their intention clear to vote for candidates 2, 4 and 5, by marking the 'circle' alongside their name with a conventional method of ranking up to three candidates, the maximum allowed

STV ELECTIONS

1



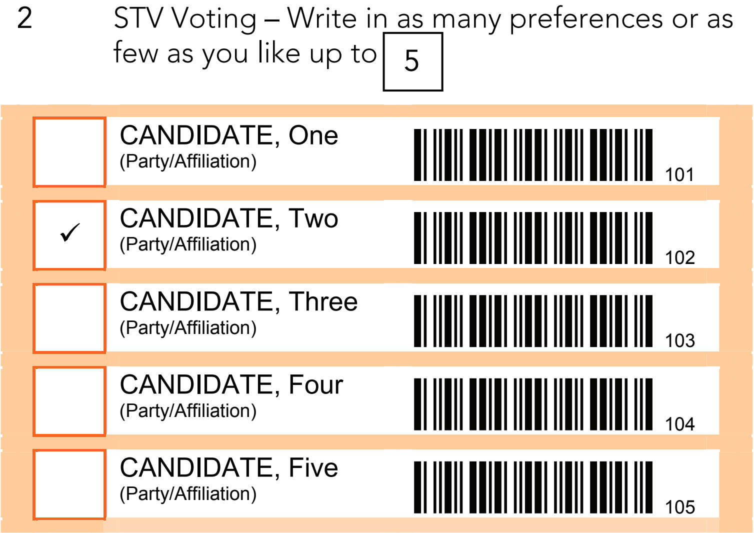
STV Voting – Write in as many preferences or as few as you like up to 5

2	CANDIDATE, One (Party/Affiliation)	101
1	CANDIDATE, Two (Party/Affiliation)	102
3	CANDIDATE, Three (Party/Affiliation)	103
5	CANDIDATE, Four (Party/Affiliation)	104
4	CANDIDATE, Five (Party/Affiliation)	105

Allow

Voter has voted for all 5 candidates and clearly indicated preferences from 1 to 5

2



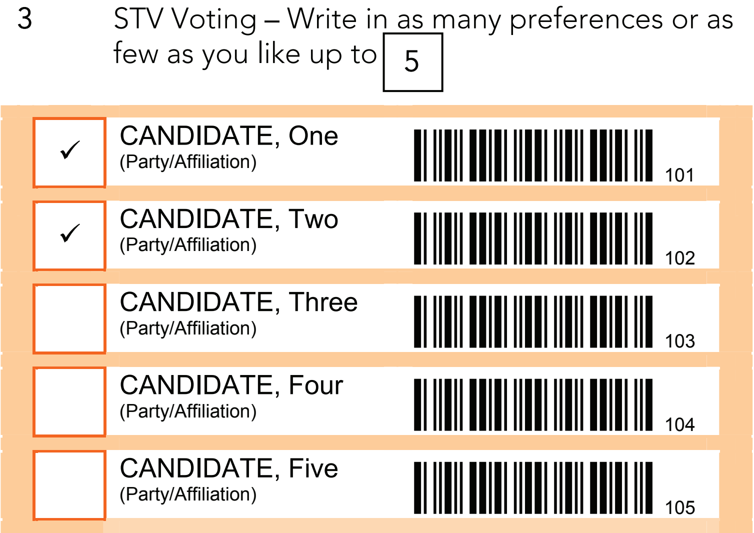
STV Voting – Write in as many preferences or as few as you like up to 5

	CANDIDATE, One (Party/Affiliation)	101
✓	CANDIDATE, Two (Party/Affiliation)	102
	CANDIDATE, Three (Party/Affiliation)	103
	CANDIDATE, Four (Party/Affiliation)	104
	CANDIDATE, Five (Party/Affiliation)	105

Allow

The voter has indicated intention to vote for one candidate as their only unique clear preference

3



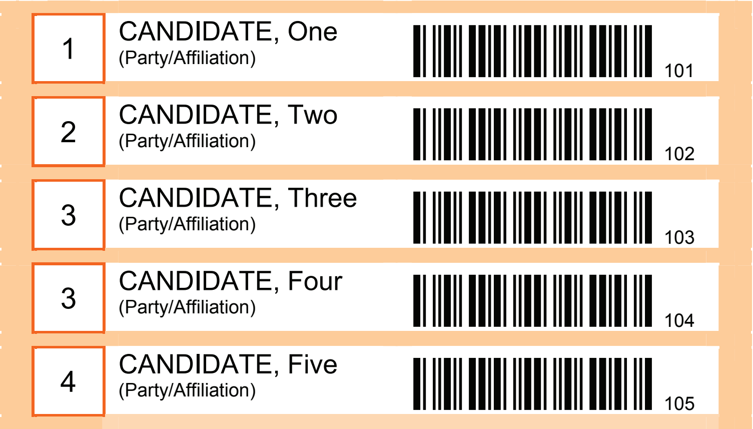
STV Voting – Write in as many preferences or as few as you like up to 5

✓	CANDIDATE, One (Party/Affiliation)	101
✓	CANDIDATE, Two (Party/Affiliation)	102
	CANDIDATE, Three (Party/Affiliation)	103
	CANDIDATE, Four (Party/Affiliation)	104
	CANDIDATE, Five (Party/Affiliation)	105

Disallow as Informal

Voter does not clearly indicate their unique first preference between candidates 1 and 2 by ticking them both

4 STV Voting – Write in as many preferences or as few as you like up to 5



1	CANDIDATE, One (Party/Affiliation)	101
2	CANDIDATE, Two (Party/Affiliation)	102
3	CANDIDATE, Three (Party/Affiliation)	103
3	CANDIDATE, Four (Party/Affiliation)	104
4	CANDIDATE, Five (Party/Affiliation)	105

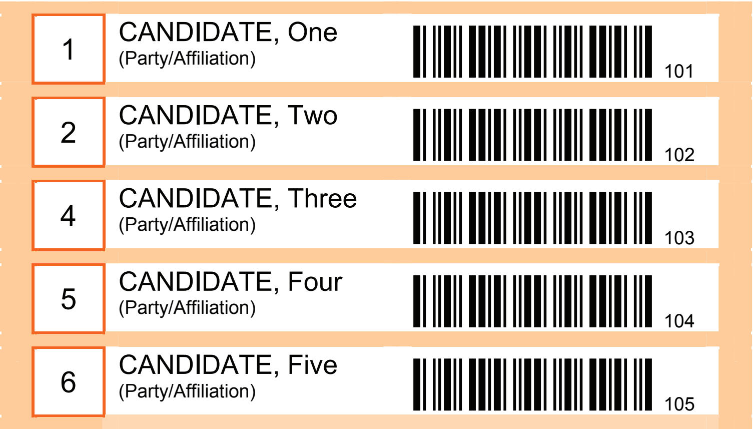
Allow

Voter's preferences for candidates 1 and 2

Disallow

Voter's other preferences because unable to determine a third unique preference between candidates 3 and 4

5 STV Voting – Write in as many preferences or as few as you like up to 5



1	CANDIDATE, One (Party/Affiliation)	101
2	CANDIDATE, Two (Party/Affiliation)	102
4	CANDIDATE, Three (Party/Affiliation)	103
5	CANDIDATE, Four (Party/Affiliation)	104
6	CANDIDATE, Five (Party/Affiliation)	105

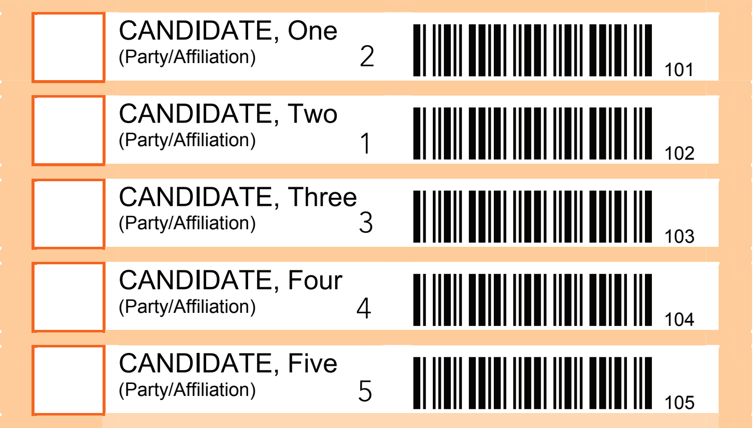
Allow

Voter's preferences for 1 and 2

Disallow

Other preferences because no third unique preference is indicated by the voter

6 STV Voting – Write in as many preferences or as few as you like up to 5

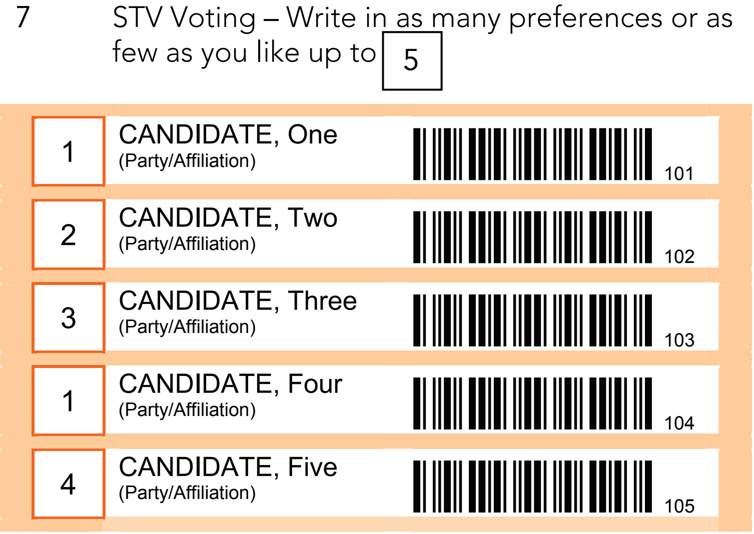


	CANDIDATE, One (Party/Affiliation)	2	101
	CANDIDATE, Two (Party/Affiliation)	1	102
	CANDIDATE, Three (Party/Affiliation)	3	103
	CANDIDATE, Four (Party/Affiliation)	4	104
	CANDIDATE, Five (Party/Affiliation)	5	105

Allow

Although the voter has not placed their preferences in the 'box', they have voted for all five candidates and clearly indicate their preferences from 1 to 5

7



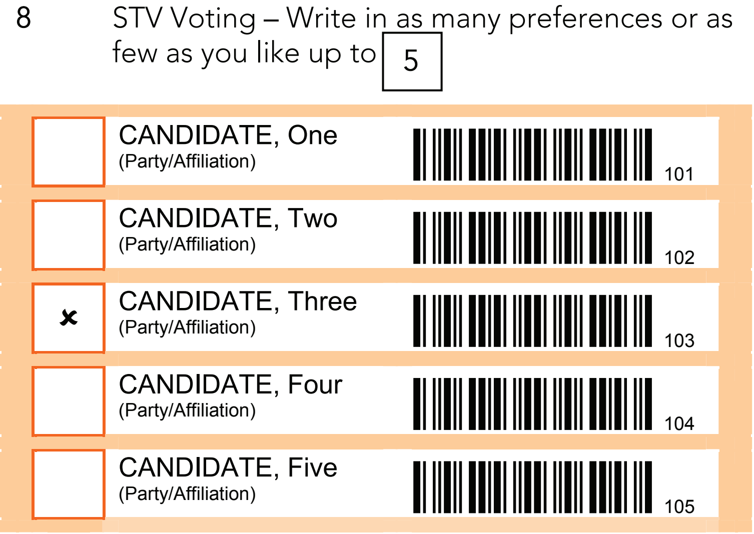
STV Voting – Write in as many preferences or as few as you like up to 5

1	CANDIDATE, One (Party/Affiliation)	101
2	CANDIDATE, Two (Party/Affiliation)	102
3	CANDIDATE, Three (Party/Affiliation)	103
1	CANDIDATE, Four (Party/Affiliation)	104
4	CANDIDATE, Five (Party/Affiliation)	105

Disallow as Informal

The voter has not distinguished an unique first preference between candidates 1 and 4

8



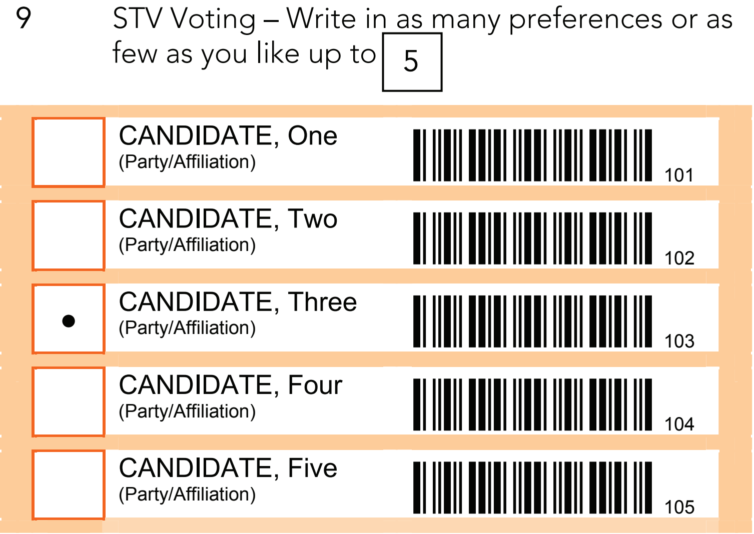
STV Voting – Write in as many preferences or as few as you like up to 5

	CANDIDATE, One (Party/Affiliation)	101
	CANDIDATE, Two (Party/Affiliation)	102
✗	CANDIDATE, Three (Party/Affiliation)	103
	CANDIDATE, Four (Party/Affiliation)	104
	CANDIDATE, Five (Party/Affiliation)	105

Allow

The voter has attempted to indicate their intention to vote for candidate 3 as their unique first and only preference

9



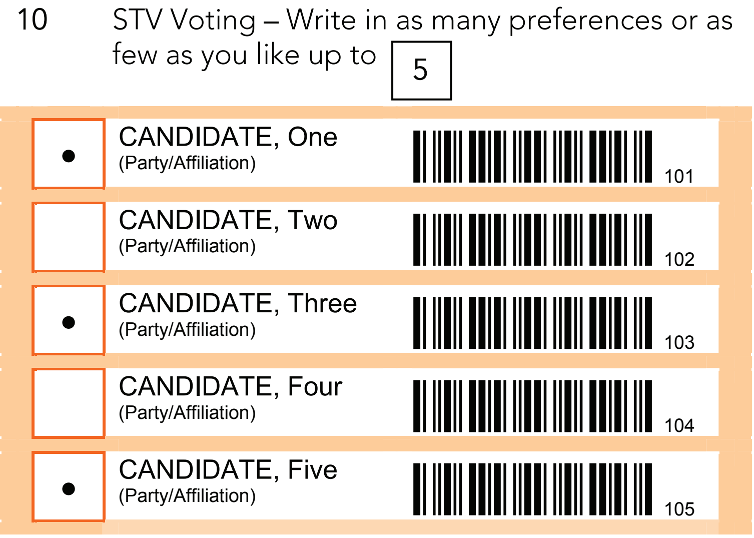
STV Voting – Write in as many preferences or as few as you like up to 5

	CANDIDATE, One (Party/Affiliation)	101
	CANDIDATE, Two (Party/Affiliation)	102
●	CANDIDATE, Three (Party/Affiliation)	103
	CANDIDATE, Four (Party/Affiliation)	104
	CANDIDATE, Five (Party/Affiliation)	105

Allow

The voter has attempted to indicate their intention to vote for candidate 3 as their unique first and only preference

10



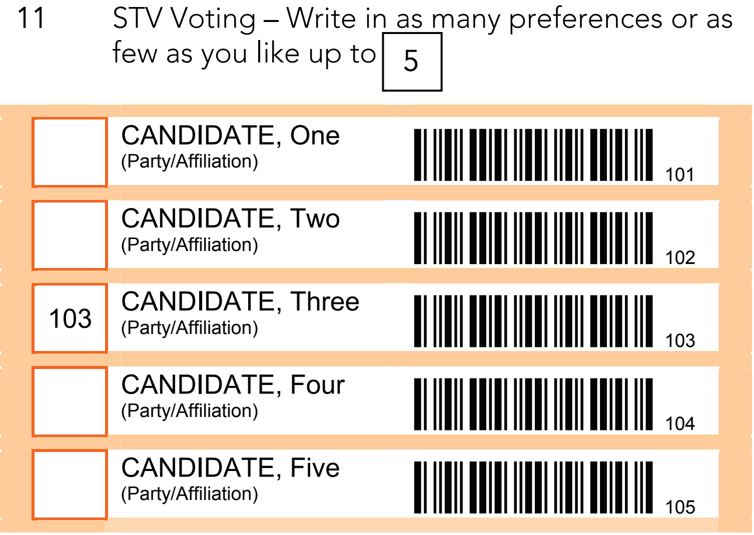
STV Voting – Write in as many preferences or as few as you like up to 5

●	CANDIDATE, One (Party/Affiliation)	101
	CANDIDATE, Two (Party/Affiliation)	102
●	CANDIDATE, Three (Party/Affiliation)	103
	CANDIDATE, Four (Party/Affiliation)	104
●	CANDIDATE, Five (Party/Affiliation)	105

Disallow as Informal

The voter has not shown a unique first preference for any of the candidates they intended to vote for

11



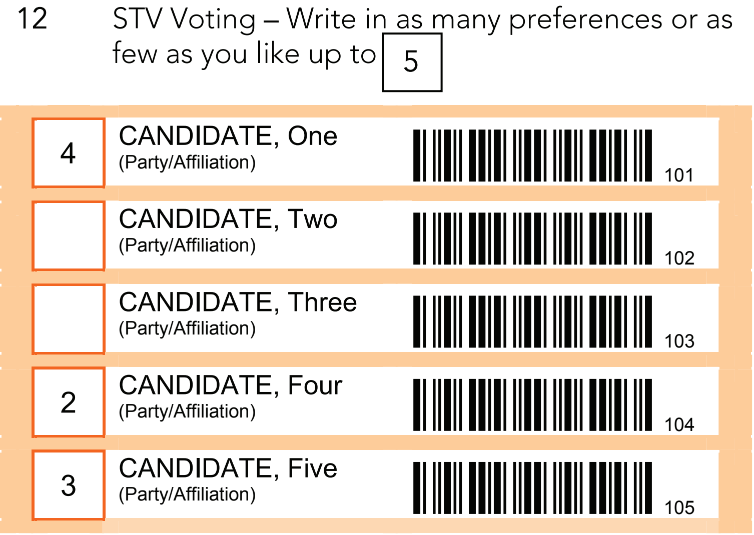
STV Voting – Write in as many preferences or as few as you like up to 5

	CANDIDATE, One (Party/Affiliation)	101
	CANDIDATE, Two (Party/Affiliation)	102
103	CANDIDATE, Three (Party/Affiliation)	103
	CANDIDATE, Four (Party/Affiliation)	104
	CANDIDATE, Five (Party/Affiliation)	105

Allow

The voter has attempted to indicate their intention to vote for candidate 3 as their unique first and only preference by writing in that candidate's readable barcode number

12



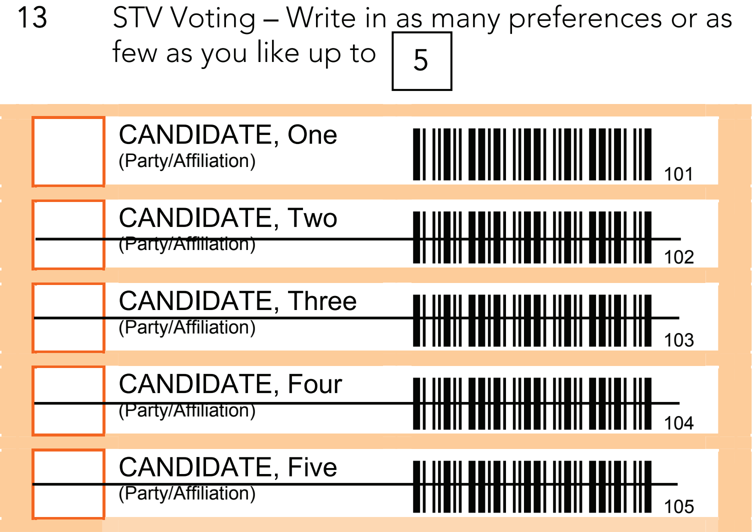
STV Voting – Write in as many preferences or as few as you like up to 5

4	CANDIDATE, One (Party/Affiliation)	101
	CANDIDATE, Two (Party/Affiliation)	102
	CANDIDATE, Three (Party/Affiliation)	103
2	CANDIDATE, Four (Party/Affiliation)	104
3	CANDIDATE, Five (Party/Affiliation)	105

Disallow as Informal

The voter has not indicated their unique first preference

13



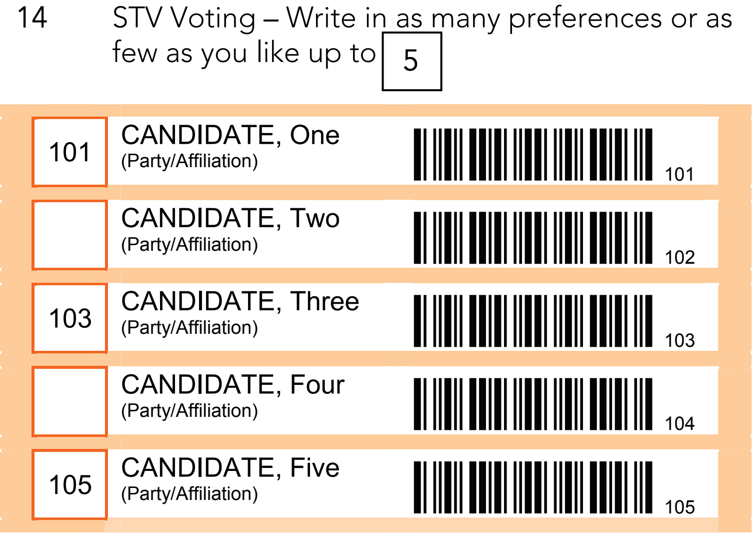
STV Voting – Write in as many preferences or as few as you like up to 5

	CANDIDATE, One (Party/Affiliation)	101
	~~CANDIDATE, Two (Party/Affiliation)~~	102
	~~CANDIDATE, Three (Party/Affiliation)~~	103
	~~CANDIDATE, Four (Party/Affiliation)~~	104
	~~CANDIDATE, Five (Party/Affiliation)~~	105

Allow

The voter has attempted to indicate their intention to vote for candidate 1 as their unique first and only preference

14



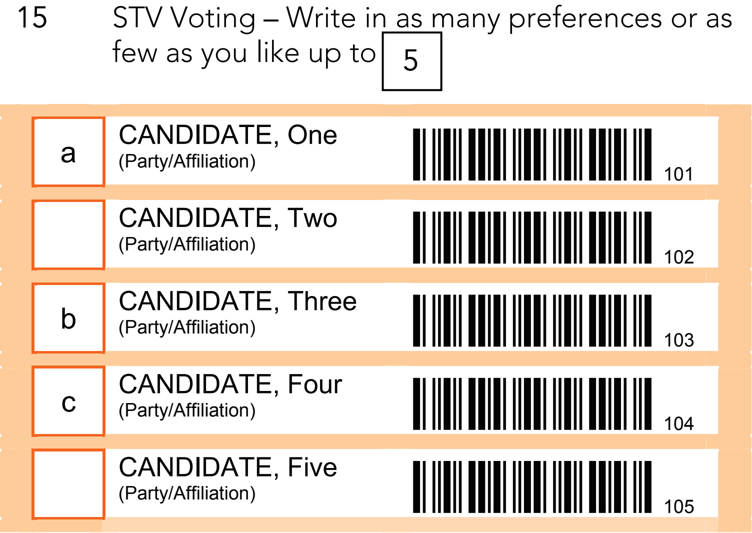
STV Voting – Write in as many preferences or as few as you like up to 5

101	CANDIDATE, One (Party/Affiliation)	101
	CANDIDATE, Two (Party/Affiliation)	102
103	CANDIDATE, Three (Party/Affiliation)	103
	CANDIDATE, Four (Party/Affiliation)	104
105	CANDIDATE, Five (Party/Affiliation)	105

Disallow as Informal

The voter has not indicated a unique first preference for any of the three candidates they have voted for

15

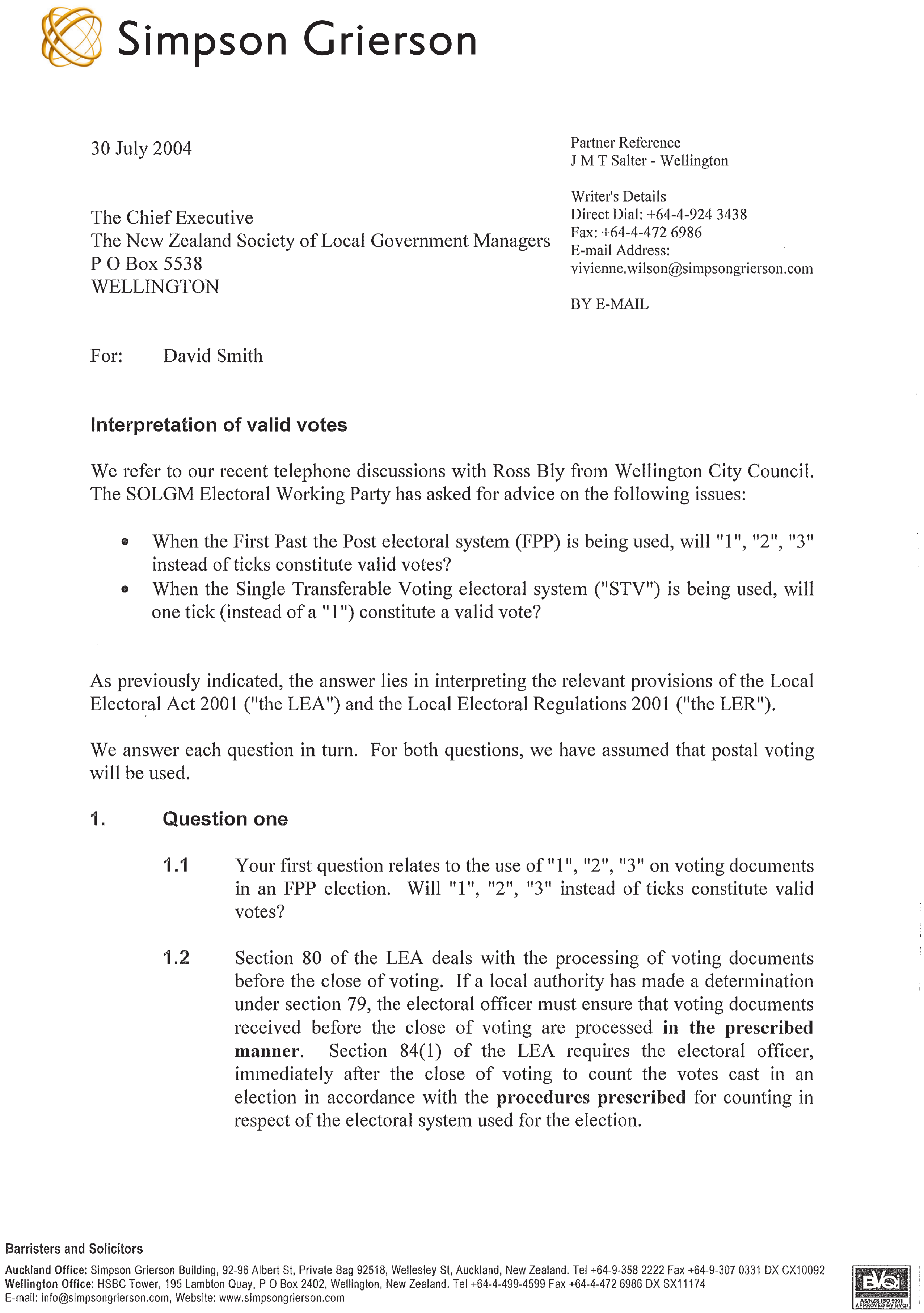


STV Voting – Write in as many preferences or as few as you like up to 5

a	CANDIDATE, One (Party/Affiliation)	101
	CANDIDATE, Two (Party/Affiliation)	102
b	CANDIDATE, Three (Party/Affiliation)	103
c	CANDIDATE, Four (Party/Affiliation)	104
	CANDIDATE, Five (Party/Affiliation)	105

Allow

The voter has attempted to show their unique first preference and subsequent preferences for three candidates using the commonly accepted ranking of a, b, c



Simpson Grierson

30 July 2004

Partner Reference
J M T Salter - Wellington

Writer's Details
Direct Dial: +64-4-924 3438
Fax: +64-4-472 6986
E-mail Address:
vivienne.wilson@simpsongrierson.com

BY E-MAIL

The Chief Executive
The New Zealand Society of Local Government Managers
P O Box 5538
WELLINGTON

For: David Smith

Interpretation of valid votes

We refer to our recent telephone discussions with Ross Bly from Wellington City Council. The SOLGM Electoral Working Party has asked for advice on the following issues:

- When the First Past the Post electoral system (FPP) is being used, will "1", "2", "3" instead of ticks constitute valid votes?
- When the Single Transferable Voting electoral system ("STV") is being used, will one tick (instead of a "1") constitute a valid vote?

As previously indicated, the answer lies in interpreting the relevant provisions of the Local Electoral Act 2001 ("the LEA") and the Local Electoral Regulations 2001 ("the LER").

We answer each question in turn. For both questions, we have assumed that postal voting will be used.

1. Question one

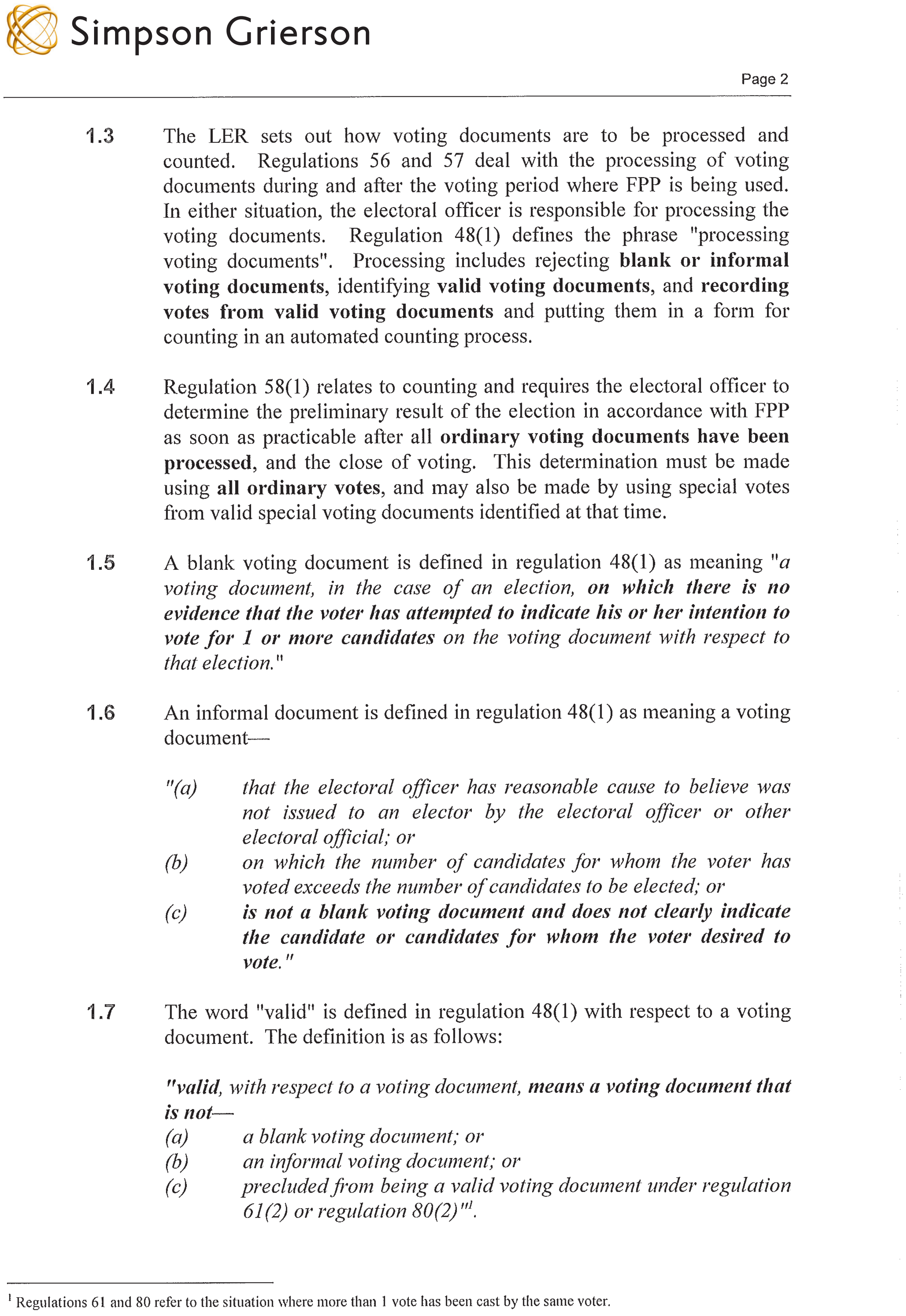
1.1 Your first question relates to the use of "1", "2", "3" on voting documents in an FPP election. Will "1", "2", "3" instead of ticks constitute valid votes?

1.2 Section 80 of the LEA deals with the processing of voting documents before the close of voting. If a local authority has made a determination under section 79, the electoral officer must ensure that voting documents received before the close of voting are processed **in the prescribed manner**. Section 84(1) of the LEA requires the electoral officer, immediately after the close of voting to count the votes cast in an election in accordance with the **procedures prescribed** for counting in respect of the electoral system used for the election.

Barristers and Solicitors

Auckland Office: Simpson Grierson Building, 92-96 Albert St, Private Bag 92518, Wellesley St, Auckland, New Zealand. Tel +64-9-358 2222 Fax +64-9-307 0331 DX CX10092
Wellington Office: HSBC Tower, 195 Lambton Quay, P O Box 2402, Wellington, New Zealand. Tel +64-4-499-4599 Fax +64-4-472 6986 DX SX11174
E-mail: info@simpsongrierson.com, Website: www.simpsongrierson.com

BVQI AS/NZS ISO 9001 APPROVED BY BVQI



1.3 The LER sets out how voting documents are to be processed and counted. Regulations 56 and 57 deal with the processing of voting documents during and after the voting period where FPP is being used. In either situation, the electoral officer is responsible for processing the voting documents. Regulation 48(1) defines the phrase "processing voting documents". Processing includes rejecting **blank or informal voting documents**, identifying **valid voting documents**, and **recording votes from valid voting documents** and putting them in a form for counting in an automated counting process.

1.4 Regulation 58(1) relates to counting and requires the electoral officer to determine the preliminary result of the election in accordance with FPP as soon as practicable after all **ordinary voting documents have been processed**, and the close of voting. This determination must be made using **all ordinary votes**, and may also be made by using special votes from valid special voting documents identified at that time.

1.5 A blank voting document is defined in regulation 48(1) as meaning "*a voting document, in the case of an election,* ***on which there is no evidence that the voter has attempted to indicate his or her intention to vote for 1 or more candidates*** *on the voting document with respect to that election.*"

1.6 An informal document is defined in regulation 48(1) as meaning a voting document—

"*(a) that the electoral officer has reasonable cause to believe was not issued to an elector by the electoral officer or other electoral official; or*

(b) on which the number of candidates for whom the voter has voted exceeds the number of candidates to be elected; or

(c) ***is not a blank voting document and does not clearly indicate the candidate or candidates for whom the voter desired to vote.***"

1.7 The word "valid" is defined in regulation 48(1) with respect to a voting document. The definition is as follows:

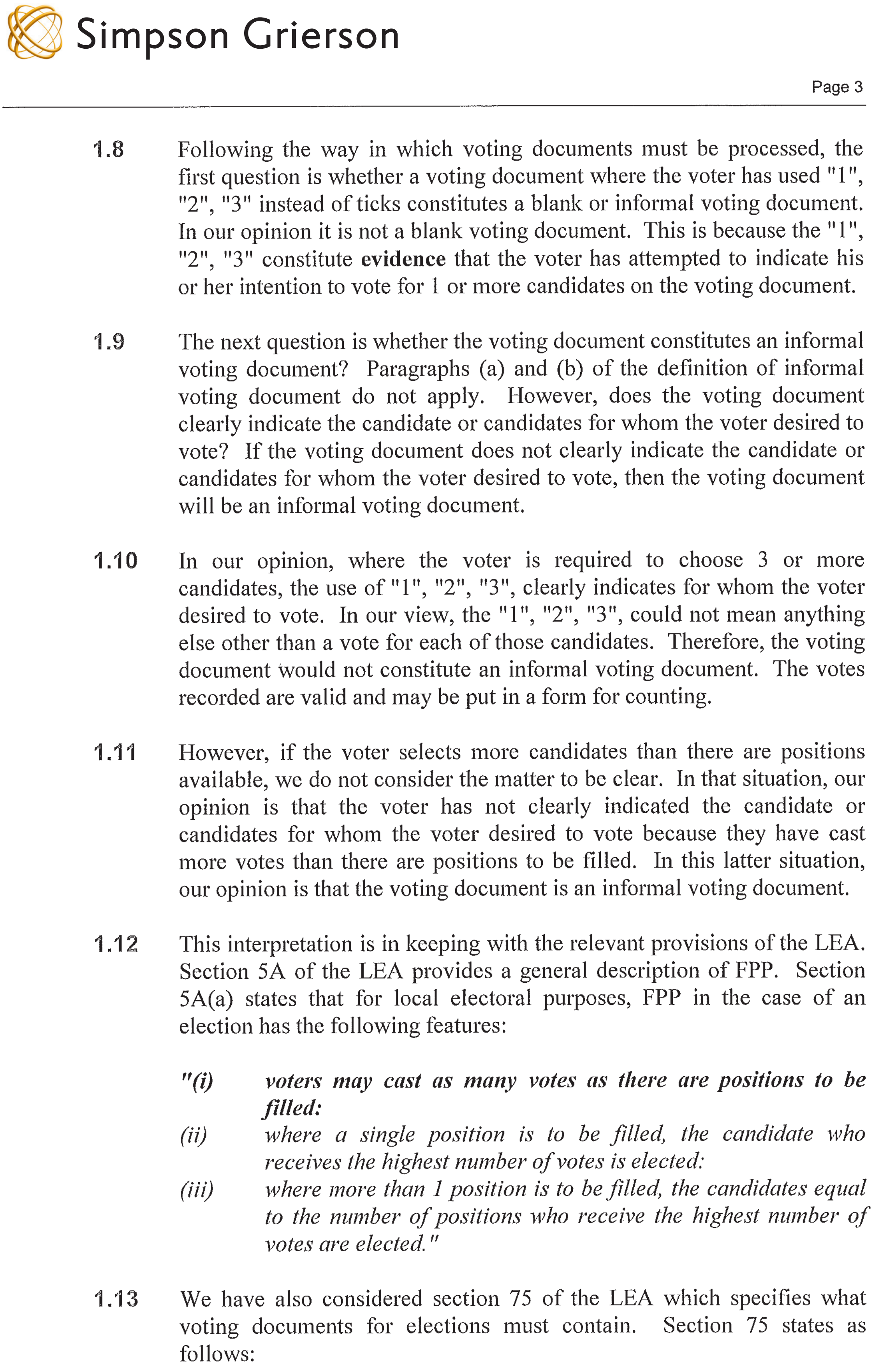
"***valid****, with respect to a voting document,* ***means a voting document that is not—***

(a) a blank voting document; or

(b) an informal voting document; or

(c) precluded from being a valid voting document under regulation 61(2) or regulation 80(2)"[1].

[1] Regulations 61 and 80 refer to the situation where more than 1 vote has been cast by the same voter.



1.8 Following the way in which voting documents must be processed, the first question is whether a voting document where the voter has used "1", "2", "3" instead of ticks constitutes a blank or informal voting document. In our opinion it is not a blank voting document. This is because the "1", "2", "3" constitute **evidence** that the voter has attempted to indicate his or her intention to vote for 1 or more candidates on the voting document.

1.9 The next question is whether the voting document constitutes an informal voting document? Paragraphs (a) and (b) of the definition of informal voting document do not apply. However, does the voting document clearly indicate the candidate or candidates for whom the voter desired to vote? If the voting document does not clearly indicate the candidate or candidates for whom the voter desired to vote, then the voting document will be an informal voting document.

1.10 In our opinion, where the voter is required to choose 3 or more candidates, the use of "1", "2", "3", clearly indicates for whom the voter desired to vote. In our view, the "1", "2", "3", could not mean anything else other than a vote for each of those candidates. Therefore, the voting document would not constitute an informal voting document. The votes recorded are valid and may be put in a form for counting.

1.11 However, if the voter selects more candidates than there are positions available, we do not consider the matter to be clear. In that situation, our opinion is that the voter has not clearly indicated the candidate or candidates for whom the voter desired to vote because they have cast more votes than there are positions to be filled. In this latter situation, our opinion is that the voting document is an informal voting document.

1.12 This interpretation is in keeping with the relevant provisions of the LEA. Section 5A of the LEA provides a general description of FPP. Section 5A(a) states that for local electoral purposes, FPP in the case of an election has the following features:

> "(i) ***voters may cast as many votes as there are positions to be filled:***
>
> (ii) *where a single position is to be filled, the candidate who receives the highest number of votes is elected:*
>
> (iii) *where more than 1 position is to be filled, the candidates equal to the number of positions who receive the highest number of votes are elected."*

1.13 We have also considered section 75 of the LEA which specifies what voting documents for elections must contain. Section 75 states as follows:

> "(1) *Every voting document for an election must contain the following directions to the voter:*
>
> *(a) the voter should read the directions carefully before voting; and*
>
> *(b) if the First Past the Post electoral system is being used at the election,—*
>
> ***(i) how and where on the voting document a voter exercises his or her vote (for example, a tick against a box); and***
>
> *(ii) the minimum and maximum number of candidates for which a voter may exercise his or her vote; and*
>
> (2) *In addition to the directions to the voter, every voting document for an election must contain the following:*
>
> ...
>
> ***(f) an illustration of how and where the voter indicates his or her choice or preferences, as the case may be."***

1.14 Section 75 requires the directions to the voter on the voting document to include how and where on the voting document a voter exercise his or her vote. This section gives a specific example of a tick against a box. However, we do not consider that this means that a voter must always use a tick against a box. A tick is simply an example.

1.15 Consequently, in our opinion "1", "2", "3" instead of ticks will constitute valid votes where there are 3 or more positions to be filled.

2. Question two

2.1 Your second question relates to the use of a tick on voting documents in a STV election. Will one tick (instead of a "1") constitute a valid vote?

2.2 Again, the starting point is the LEA and the LER. Regulations 101 and 102 deal with the processing of voting documents during and after the voting period where STV is being used. In either situation, the electoral officer is responsible for processing the voting documents. Regulation 91(1) defines the phrase "processing voting documents". Processing includes rejecting **blank or informal voting documents**, identifying **valid voting documents**, and **recording votes from valid voting documents** and putting them in a form for counting by a certified counting program.

2.3 Regulation 103(1) relates to counting and requires the electoral officer to determine the preliminary result of the election using a certified counting program as soon as practicable after all **ordinary voting documents have been processed**, and the close of voting. This determination must be made using **all ordinary votes**, and may also be made by using special votes from valid special voting documents identified at that time.

2.4 A blank voting document is defined in regulation 91(1) as meaning "*a voting document, in the case of an election,* ***on which there is no evidence that the voter has attempted to indicate his or her intention to vote for 1 or more candidates*** *on the voting document with respect to that election.*"

2.5 An informal document is defined in regulation 91(1) as meaning a voting document—

"*(a) that the electoral officer has reasonable cause to believe was not issued to an elector by the electoral officer or other electoral official; or*

(b) ***is not a blank voting document and does not clearly indicate the voter's first unique preference.***"

2.6 The word "valid" is defined in regulation 91(1) with respect to a voting document. The definition is as follows:

"***valid****, with respect to a voting document,* ***means a voting document that is not***—

(a) a blank voting document; or

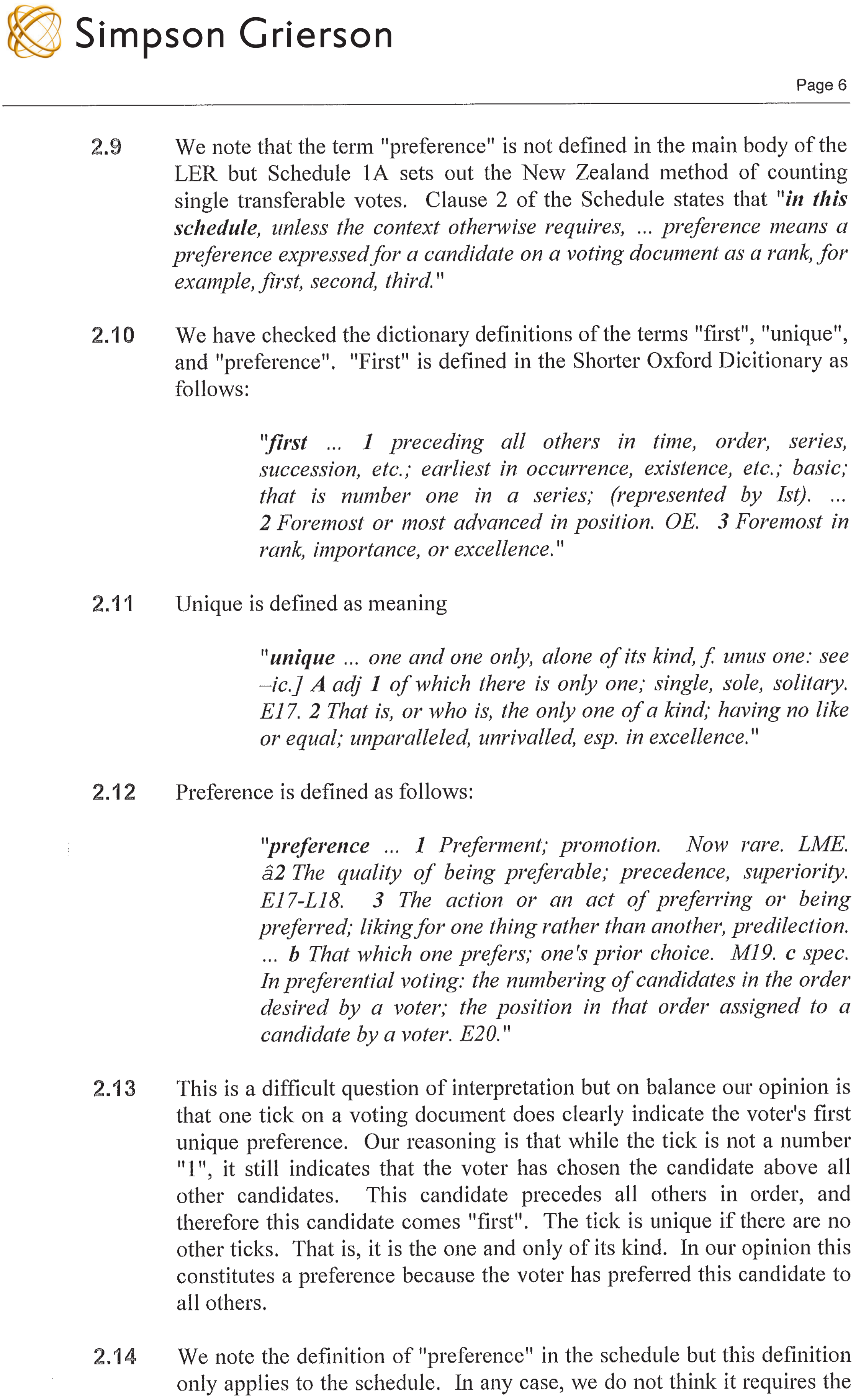
(b) an informal voting document; or

(c) precluded from being a valid voting document under regulation 105(2) or regulation 125(2)"[2].

2.7 Again, following the way in which voting documents must be processed, the first question is whether a voting document where the voter has used a tick instead of a "1" constitutes a blank or informal voting document. In our opinion it is not a blank voting document. This is because the tick constitutes **evidence** that the voter has attempted to indicate his or her intention to vote for 1 or more candidates on the voting document.

2.8 The next question is whether the voting document constitutes an informal voting document. Again paragraph (a) of the definition of informal voting document does not apply. However, does the voting document clearly indicate the voter's unique first preference as stated in paragraph (b)? We note that paragraph (b) was recently amended by the Local Electoral Amendment Act 2003. Prior to the amendment, paragraph (b) stated "*is not a blank voting document and does not clearly indicate any recognisable preference for any candidate*".

[2] Regulations 105 and 125 refer to the situation where more than 1 vote has been cast by the same voter.



2.9 We note that the term "preference" is not defined in the main body of the LER but Schedule 1A sets out the New Zealand method of counting single transferable votes. Clause 2 of the Schedule states that "***in this schedule***, *unless the context otherwise requires, ... preference means a preference expressed for a candidate on a voting document as a rank, for example, first, second, third.*"

2.10 We have checked the dictionary definitions of the terms "first", "unique", and "preference". "First" is defined in the Shorter Oxford Dicitionary as follows:

> "***first*** *... **1** preceding all others in time, order, series, succession, etc.; earliest in occurrence, existence, etc.; basic; that is number one in a series; (represented by Ist). ... **2** Foremost or most advanced in position. OE. **3** Foremost in rank, importance, or excellence.*"

2.11 Unique is defined as meaning

> "***unique*** *... one and one only, alone of its kind, f. unus one: see –ic.] **A** adj **1** of which there is only one; single, sole, solitary. E17. **2** That is, or who is, the only one of a kind; having no like or equal; unparalleled, unrivalled, esp. in excellence.*"

2.12 Preference is defined as follows:

> "***preference*** *... **1** Preferment; promotion. Now rare. LME. â**2** The quality of being preferable; precedence, superiority. E17-L18. **3** The action or an act of preferring or being preferred; liking for one thing rather than another, predilection. ... **b** That which one prefers; one's prior choice. M19. **c** spec. In preferential voting: the numbering of candidates in the order desired by a voter; the position in that order assigned to a candidate by a voter. E20.*"

2.13 This is a difficult question of interpretation but on balance our opinion is that one tick on a voting document does clearly indicate the voter's first unique preference. Our reasoning is that while the tick is not a number "1", it still indicates that the voter has chosen the candidate above all other candidates. This candidate precedes all others in order, and therefore this candidate comes "first". The tick is unique if there are no other ticks. That is, it is the one and only of its kind. In our opinion this constitutes a preference because the voter has preferred this candidate to all others.

2.14 We note the definition of "preference" in the schedule but this definition only applies to the schedule. In any case, we do not think it requires the use of a "1". What is important is the ranking of candidates and where only one tick has been placed next to one candidate that candidate has been ranked ahead of all others.

2.15 Therefore, our opinion is that the voting document would not constitute an informal voting document and that the vote may be put in a form for counting by a certified counting program.

2.16 For completion, we note that if a voting document was to include two or more ticks, the voting document would be informal because it would not clearly indicate the voter's first unique preference.

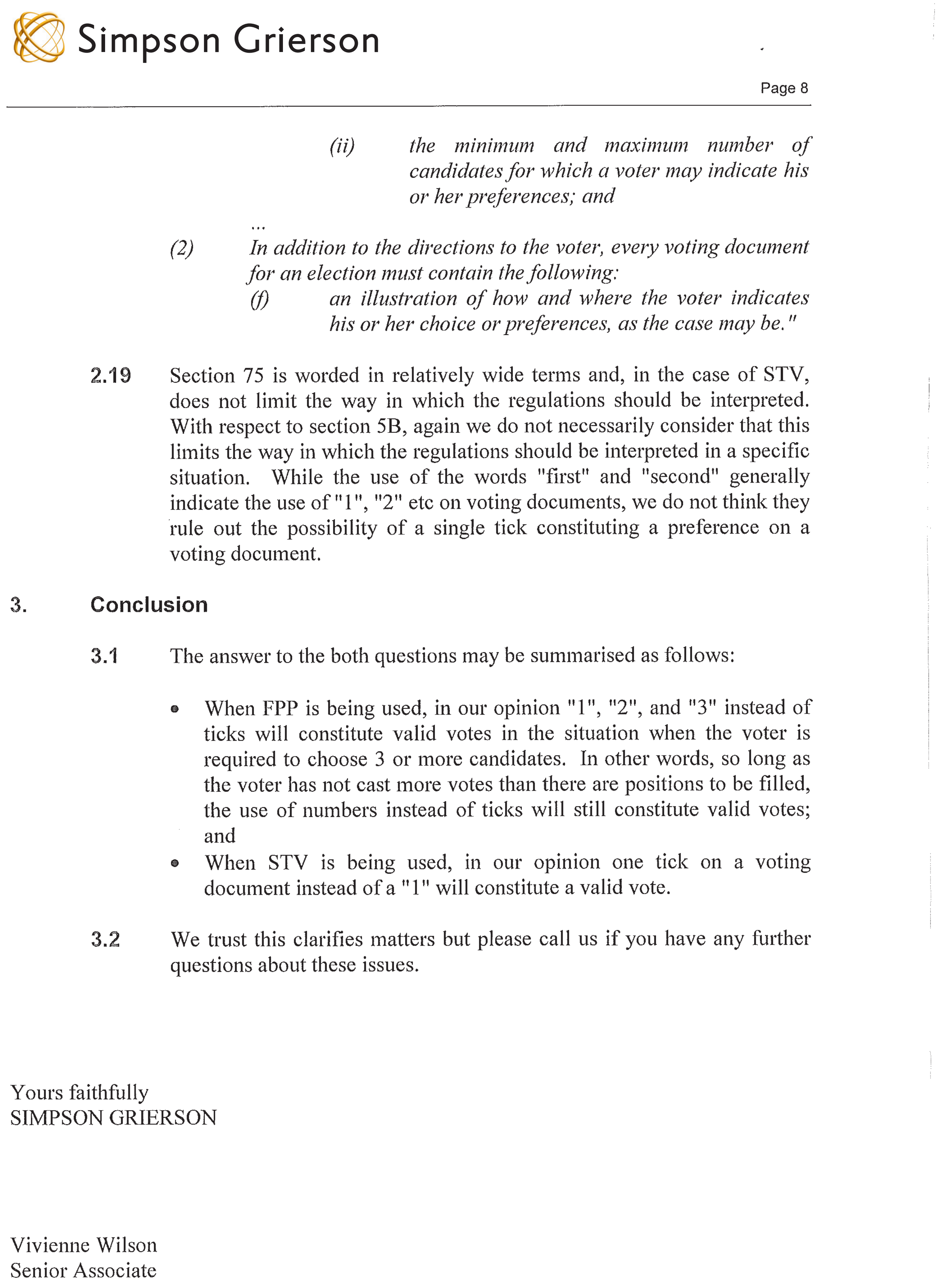
2.17 Again, we consider that this interpretation is not at odds with the relevant provisions of the LEA. Section 5B of the LEA provides a general description of STV. Section 5B(a) states that for local electoral purposes, STV, in the case of an election for multi-member vacancies has the following features:

"*(i)* ***voters express a first preference for 1 candidate and may express second and further preferences for other candidates****:*
(ii) a quota for election is calculated from the number of votes and positions to be filled:
(iii) the first preferences are counted and any candidate whose first preference votes equal or exceed the quota is elected:
(iv) if insufficient candidates are elected under subparagraph (iii), the proportion of an elected candidate's votes above the quota is redistributed according to voters' further preferences, and—
(A) candidates who then reach the quota are elected; and
(B) the candidate with the fewest votes is excluded:
(v) the excluded candidate's votes are redistributed according to voters' further preferences:
(vi) if insufficient candidates are elected under subparagraphs (iv) and (v), the steps described in subparagraphs (iv) and (v) are repeated until all positions are filled:"

2.18 We also note that section 75 of the LEA dealing with voting documents states that:

"***What voting documents for election must contain—***

(1) Every voting document for an election must contain the following directions to the voter:
...
(c) if the Single Transferable Voting electoral system is being used at the election,—
(i) how and where on the voting document a voter indicates his or her preferences; and



> (ii) *the minimum and maximum number of candidates for which a voter may indicate his or her preferences; and*
>
> ...
>
> (2) *In addition to the directions to the voter, every voting document for an election must contain the following:*
>
> (*f*) *an illustration of how and where the voter indicates his or her choice or preferences, as the case may be."*

2.19 Section 75 is worded in relatively wide terms and, in the case of STV, does not limit the way in which the regulations should be interpreted. With respect to section 5B, again we do not necessarily consider that this limits the way in which the regulations should be interpreted in a specific situation. While the use of the words "first" and "second" generally indicate the use of "1", "2" etc on voting documents, we do not think they rule out the possibility of a single tick constituting a preference on a voting document.

3. Conclusion

3.1 The answer to the both questions may be summarised as follows:

- When FPP is being used, in our opinion "1", "2", and "3" instead of ticks will constitute valid votes in the situation when the voter is required to choose 3 or more candidates. In other words, so long as the voter has not cast more votes than there are positions to be filled, the use of numbers instead of ticks will still constitute valid votes; and
- When STV is being used, in our opinion one tick on a voting document instead of a "1" will constitute a valid vote.

3.2 We trust this clarifies matters but please call us if you have any further questions about these issues.

Yours faithfully
SIMPSON GRIERSON

Vivienne Wilson
Senior Associate

SOLGM
NEW ZEALAND SOCIETY OF
LOCAL GOVERNMENT MANAGERS

PART 15: APPENDIX B
MANAGING THE ELECTRONIC INFORMATION

CONTENTS

INTRODUCTION

Current practice in New Zealand is to use electronic information systems to run local authority elections. Data is captured into databases, verified, corrected and then used to calculate results.

In addition to legal compliance the running of a successful election, when using a computer system, relies on the application of professional standards and processes in all aspects of the election process. Often, those standards are maintained by professional information technology (IT) personnel.

This document identifies the legal framework and recommends best practice for a range of IT issues. Some factors are described in depth, while others are not. In either case, the document catalogues the factors that the electoral officer (EO) needs to be aware of and discuss with their IT professional if they have one.

The document describes the risks to running a successful election posed by an information system that fails or is compromised by persons within or outside the EO's team.

The document applies equally to elections run under FPP and STV, with the exception that under STV, the result of each election must be calculated using the certified STV calculator provided by the Department of Internal Affairs.

For definitive information about STV elections, refer to *Schedule 1 of the Local Electoral Act 2001 (LEA)*. Further information can be found from www.stv.govt.nz

OBJECTIVE

The objectives of this document are:

1. to make the EOs aware of the IT issues and risks to be considered when using a computer network to help run an election;

2. to clarify the procedures required by legislation when using a computer system to electronically record and count votes.

LEGISLATION

Local Electoral Act 2001

Section 139 of the *LEA* prescribes what Regulations may cover. This includes the use of electoral rolls, generally, and also the prescribing standards, performance measures, procedures, and forms for the conduct of elections or polls. All of the conditions and restrictions involving recording and counting software are found in the Regulations.

Where sections of the *LEA* or *Local Electoral Regulations 2001 (LER)* have been illustrated in this document, these should be taken as a guide only and are not intended to replace any of the wording of the *LEA* or *LER* as published. Nor does any interpretation of the *LEA* or *LER* in this document necessarily arise from a legal opinion.

Local Electoral Regulations 2001

Key regulations affecting the use of a computer system are:

Regulation 31	*Order of candidates names on voting documents*
For FPP elections	
Regulation 56	*Processing voting documents during voting period*
Regulation 57	*Processing voting documents after voting period*
Regulation 58	*Counting votes*
Regulation 59	*Checking systems*
Regulation 60	*Performance standard for checking systems*

For STV elections

Regulation 91	*Interpretation*
Regulation 101	*Processing voting documents during voting period*
Regulation 102	*Processing voting documents after voting period*
Regulation 103	*Counting votes*
Regulation 104	*Checking systems*
Regulation 104A	*Performance standard for checking systems*

RECOMMENDED PRACTICES

Physical security

Server

If the server is not located at the election office, find out where it is located and ensure that physical access to it is restricted and secure. Find out who has authorised access. These persons will need to be aware of the election timetable so that the server is not removed from service at critical times.

Maintain a list of authorised users of the server.

Have one main contact person from the IT team and keep that person informed.

Workstations

The workstations (PCs) need to be located in an area accessible by only authorised persons at all times.

Backups

Ensure that backups that are taken regularly from the database are stored safely and securely offsite away from the server itself so that the server and its backups cannot be damaged or destroyed simultaneously.

Maintain a backup log

A fire-proof safe should be used for storage of backup media with security access being carefully controlled.

Offsite storage companies can be employed with transportation of media being via a secure courier. One-hour return should be available.

Backups should be securely erased or destroyed after the election. Backup tapes should be destroyed, not simply discarded or reused. Backups made to a hard disk system are not fully erased until the data is overwritten with null or other data. Deleting the files is not sufficient. This is especially important when a rented server is returned to the supplier.

Network security

Connection to the Internet

Your very best strategy is not to have your election computer network connected to the Internet or to any other corporate network. If you have a choice, this is the safest approach from a security point of view. In particular, there should be no wireless access to the election network.

Should you need access to email or to the Internet, you can get this through an alternative PC connected to your corporate network.

If you need to connect your election network to a wider corporate network, you should specify to your IT service provider which software applications you wish to enable on each of your networked PCs. The email server, web proxy server and firewall can be configured to allow or disallow any services that you need, without compromising your security.

Software currency

Ensure that the firewall, proxy server, email server and all other network components are completely up-to-date with security patches.

Ensure that the firewall, proxy server, email server and other devices on the network provide completely up-to-date virus protection.

Ask your IT service provider about software to detect, alert, and prevent an attack to or through the firewall.

Virus protection

Ensure that every PC in the election network is protected with an up-to-date anti-virus system.

Prevent software or documents of any sort being downloaded from the Internet or from a disc, iPod or similar device. Have all your networked PCs, other than an administration machine, configured so that portable storage devices of any sort cannot be used to copy files onto the PCs. One centralised resource drive is the best way to contain the upload of unauthorised software.

Server access

Ensure that only authorised IT administrators can log onto the server. You should have those persons sign the declaration that other election staff are required to sign.

Ensure that only nominated persons can log on to the server share that contains the database.

Network recovery

Ensure that there is a plan in place to recover from a failure in any component of the network which has the potential to stop the processing of returned voting documents. Determine the availability of spare network components.

You may need to upgrade the network infrastructure in the election office, to provide additional ports for the computers, printers and other equipment. Before this can be done, you will need a plan of the proposed layout for all your PCs, printers and other network equipment. An as-built diagram of the network will be required by an engineer to assist in identifying problems.

Single Image on network PCs

The personal computers being used in the counting process should ideally all be of the same specification and share the same configuration image, operating system and hardware profile. An image should be built and tested, then copied onto multiple machines using such software as Norton Ghost or similar. This image may be pre-loaded by a hardware rental company or by in-house technicians. The image should again be tested in a networked environment prior to Election Day. Keeping each PC identical may save you time in maintenance or fault-finding.

A backup copy of the image should be retained in the event that a re-count is required or in case the image is required as part of a scrutineering process.

Wireless networks

Wireless networks, if employed, can introduce additional security risks and should be implemented with caution, and avoided if possible. WPA security (or better) with MAC filtering should be considered a minimum standard. WEP security is not considered secure for this purpose.

Networked PC usage

Ensure that the PCs have virus protection software installed and enabled at all times and that virus definitions are up to date.

Adopt a rule that no PC operator shall insert a removable diskette, CD-ROM or any portable storage device into any PC. Under Windows/2000 or Windows/XP it is possible to restrict access of CD-ROM drives and diskette drives to the Administrator password only, thus preventing access by other users.

Ensure that the PCs cannot be used to access the Internet, or to access email programs.

PC start-up and operation

Ensure that PCs are configured so that the start-up sequence does not allow booting (start-up) from a floppy disk, CD ROM or external storage device accessed via USB or other port that may effectively compromise security.

Ensure that all PCs will automatically become locked after a few minutes without use. This is normally accomplished through the "screen saver".

Ensure all your election network users understand the rules you have established for the use of the network. If Internet access is possible from the users' PCs (which is not recommended) let them know that such usage is monitored to their PC and to their Username and ensure that this is undertaken periodically.

Usernames and passwords

Usernames and passwords for data entry operators should have been created so that the initial passwords expire at the first login for each username. Users must then choose their own private passwords.

Generic or systematic usernames (e.g. "User1") can too easily be guessed and therefore should never be used on a continuing basis.

All usernames that are not required or are no longer to be used should be removed immediately.

Passwords should conform to the council's password policies, and should meet the criteria for strong passwords (6 characters or more in length, contain a combination of letters, numbers and special characters, and not be easily to guess).

Screen-saver locks

Ensure that all PCs are configured for the screen-saver lock to activate when the PC is not used for more then 5 minutes. This will help users who may not be good at locking their PC whilst unattended. Remind your users to lock their PC - this is largely a cultural issue, make it a team priority.

Data security

Backup schedule

Discuss with your IT person when the election database will be subject to incremental and full backups.

Ensure that the backup plan never leaves you without a recent full backup of your database, even if only for a very short time. Never make a backup that overwrites your previous best backup.

Ensure that you have a full backup of the fully configured server and database before beginning the vote counting.

Document retention policy

Create a document retention plan. This is to ensure that all electronic documents or data on which the conduct of the election depends or which document the progress of the elections, are included in the backup schedule at least once per day.

Include important emails in the document retention plan.

Recovery plan and testing

Determine, in advance, how long it will take to restore the database from backups onto the same or a replacement server.

Make sure that the backup and restore process is fully tested with realistic data before voting document processing begins.

After voting document processing begins, have the IT staff restore a backup onto a test machine, and check that the data is correct.

Ensure that the server database is configured for transaction logging so that, in the event of a server failure or database corruption, data loss is minimal.

Discuss with your IT staff, how you will determine what data is in the database after recovery from a failure.

Ensure that you have adequate replacement hardware for all components of the system in case you should lose one or more components during voting document processing. Ensure that support agreements detail the response time and recovery or break-fix time and that these timeframes are appropriate.

Staff organisation

Staff checks

Ensure employees are police-checked and check references that you may have required. Where else do your employees work, are there any conflicts of interest? Data losses are often deliberate as opposed to accidental. You need to understand the triggers that cause people to act in other than your best interests.

Separation of duties

Where possible, staff duties should be separated to ensure that any person's work is checked by a different person.

The separation of duties must be supported by application software through the use of a unique logon username for each person.

Acceptance of responsibility

You will already have a non-disclosure agreement for all staff to sign relating to security of election data and processes. Extend the agreement to include destruction, damage, or attempt to invalidate any software or hardware in use for the election process. Have all staff sign this, including those with administration rights over the server and network.

Staff training

Before the early processing period begins, you should ensure that all your staff, who are unfamiliar with the election software, are trained to use it. This may require the creation of an instructional booklet if a software user's guide doesn't already exit. The guide should describe clearly and simply how to deal with the most commonly expected problems.

It is strongly recommended that you establish a training environment on your network and allow your staff to practice using it before they are required to use the production system.

PC usage

Emphasise to all staff that they must...

- Logout of their PC before leaving it unattended.
- Never share their login password with anyone else.
- Not let another person use their PC unless first logging out.

Building access

Ensure those staff employed for processing of election results have sufficient security access to the building during the period of election processing.

Where security cards are in use, ensure these are tested prior to the day/s of operation.

Communications security

Email

Access to email should be carefully controlled or simply unavailable to prevent unauthorised communication of results.

Only a single secure PC, secured to the EO's password, should have email available for communication of results to outside parties.

Internet

Where results are to be communicated via the Internet, sufficient preparation and testing of processes must have been undertaken to ensure results can be successfully presented.

Presentation of election results over the Internet could be thwarted by denial of service (DoS) attacks on the Internet server. Contingency plans are required for the dissemination of results by other methods.

The Internet server should be adequately protected with a firewall and anti virus protection, and preferably intrusion-detection software.

Printing

Access to unauthorised printer hardware outside of the electoral office should be restricted. Ideally, no printing to printers located outside the election office should be possible.

Data interchange

When any data is exchanged between computer systems operated by different organisations, (for example, data captured locally and forwarded for central processing in a DHB STV election at large), a copy should be kept of any data sent to another site, both as evidence of what was sent, and in case the consignment is lost.

At the time of writing, there is no national standard for such data interchange. The format used is the result of mutual agreement between all parties concerned.

Any data that is transferred electronically (e.g. by email or an attachment) should be followed by the data also sent on a medium such as CDROM, because electronic exchange of data may not be adequately covered by an EO's insurance policy.

Any media sent to another site should be signed and dated by the EO or his representative. The EO should also label any retained copy in the same way as the original.

Any media used for such data exchange should, if possible, be such that the data written onto it cannot be altered in any way without such alteration being clearly evident. Discuss this issue with other parties with whom you plan to exchange data. A simple, but very effective approach is to use the SH1 secure hashing process. This enables you to generate a reliable electronic signature for each data file and transmit the signature with the file.

If you are concerned about other parties intercepting and using the data you are sending, transmit the data in an encrypted form. Encrypt the data you wish to protect prior to any data interchange. Use a reliable encryption method such as Public Key Encryption. No Encryption method is entirely secure but the time taken to decrypt the data extends beyond the useful life of the data

Computer operating systems

Security updates

Ensure that the PCs and the database server are running with operating systems updated to the latest available patch level.

Compatibility

The PCs must be running an operating system compatible with the application software. In addition, the PCs on which STV results are to be calculated must be compatible with the STV calculators (main and backup calculators). The two certified DIA STV calculators require Windows 2000 or Windows XP.

System performance factors

Performance testing

Ensure that the database server provides an adequate response time with the maximum number of network PCs doing data entry simultaneously. Make sure that the software provider has done adequate testing for your particular situation. Otherwise, organise a full-load test yourself.

Server data capacity

Obtain a reasonably accurate estimate of the maximum size of your database.

Ensure that the server can accommodate your database with an adequate additional capacity. Ensure that the server has an adequate margin for the database transaction log.

Application software

Software certification

In an STV election, it is recommended that you use one of the STV calculators provided by DIA. Both STV calculators (main and backup) have been certified by an approved certifier.

Ensure that the application software package that you use for the election is also certified by a reliable certifier. If you need to, consult the DIA before signing a licence agreement. Preferably, the application software (even though in an earlier version) should have been used successfully in a previous election. Make sure that the version you are planning to use has been certified. You should ask for copies of the certificates and check them against the version numbers built into the application software.

If you receive a new version of the application software, it needs to be accompanied by an updated certificate and documentation that describes the changes made since the previous version that you have used or tested. Make sure you read the documentation and are very clear about the changes that have been made.

If you wish to test the modified software, do this first in a test or training environment.

Supplier support

Discuss with your application software supplier, the action that the supplier will take if the software fails for any reason. Have the supplier provide phone numbers for you to contact them during and after office hours, and especially around the close of voting.

Access to reporting tools

Ensure that the software components to be used to calculate and report election results are installed on only those PCs that are to be used for reporting, and that the reporting software can be run only by persons that are approved to do so. For further security, you can delay the installation of the reporting tools until just before they are required to be used, provided that the installation process has been previously tested.

If you are using election application software that contains time and password locks on the reporting tools, this should not remove the need to take further restrictive measures such as those above.

Access to intermediate files

Where intermediate files are used to link the data collection and the calculating/reporting parts of the application software, ensure that those files are held on a secure server with access limited by authorised people only.

Locking by passwords/password safety

If any part of the election application software (such as the reporting tools) is to be locked using one or more passwords, ensure that the passwords have been documented correctly, and stored in a physically secure location with restricted access. These passwords must be obtainable in an emergency. It is common practice to seal passwords in an envelope in such a way that you can clearly see when the envelope has been opened.

The use of password controlled locks on counting software is not prescribed by the *LER* or the *LEA*. It is a mechanism used in some election software to restrict access to the trends of an election while voting is in progresses. Ultimately, it is the responsibility of each EO and of all persons involved in early processing of voting documents to ensure that voting patterns are unable to be determined. Therefore, software locks should be used if they are provided by the software.

User level passwords should not be recorded anywhere, as these can be reset by the Administrator if necessary (and this should be auditable). The Administrator should not have access to election data. This is best achieved by denying the Network Administrator access to the election application software.

Data security

Persons with IT responsibility, who are assisting the EO, must take whatever steps they can to protect the recorded votes from being inspected or counted before close of voting.

On the other hand, the EO may require some assurance that votes are indeed being recorded into the database, and there is not an undetected gross malfunction of the software. The EO's IT staff may be required to generate some progressive summary statistics from the database to match against the number of voting documents known to have been processed.

Software automation

It should be possible under Windows/2000 and Windows/XP to control access to certain software applications only, with the possibility of the vote entry software being automatically started on sign-on, and sign-off being automatic on exiting this software.

Removing the ability to run other applications concurrently on the data entry PCs also reduces the chance of conflict between processes that may corrupt the vote entry process.

Results reporting

Electronic document types

Decide in advance the document types with which you will report the results and inform all the interested parties of this.

If you plan to distribute results electronically, inform the recipients of the name and version numbers of the software they will need to read your distributed documents.

Preparation of email distribution templates

At an early stage, gather lists of persons to whom you wish to send results. Build the email addresses into email templates along with the covering descriptive text. Save the templates for use after close of voting. Make sure that you test all email addresses well in advance of needing to use them.

Manual editing of results

Try to avoid having to manually edit results documents before they are distributed. If this is not possible, keep copies of all the documents before editing and at any other intermediate stages of the editing process, so that the manual process can be easily audited afterwards.

Printer hardware

Printing hardware should have been pre-installed and tested on the network where result printing is to be performed.

STV calculators

Prior testing of the main and backup STV calculators

Ensure that the process for using BOTH the main and backup calculators is determined and documented for your situation. Have both calculators installed and ready to use after the data capture is finished. In the very unlikely event of you having to use the backup calculator, make sure it can be used without delay.

You should refer to the DIA's web site www.stv.govt.nz to find the latest recommended procedures for the use of the STV calculator.

Support for the STV calculators

Details of how to obtain support for the main and backup calculators will appear on the STV web site www.stv.govt.nz. However, since the main STV calculator has been used in two triennial elections without a problem, the support available for the calculators in future elections will be minimal.

Timetable for results calculations

Work out a plan for calculating the STV issues in the required order. Use the supplied test data to obtain an estimate, on your own hardware, of the likely time to calculate each issue. If you need to, plan for running a number of STV calculators simultaneously on a number of suitably configured workstations (PCs). Have a detailed plan for making the required data available to each separate PC that will run the STV calculator. Thoroughly test the whole process with your own report templates and the best test data you have available.

Access to the STV calculator

Ensure that only a selected number of people can run the STV calculator.
Ensure that the STV calculator is installed to run only on the selected PCs in the election office and that only approved persons can log onto those PCs.

Minimum requirements to run the 'main' calculator

The following definition is from the document "STV Installation Guide v0.3.doc" from CGNZ Ltd, who supply the main calculator.

"This section outlines the minimum requirements for the STV calculator operating platform. These requirements should be met to ensure the STV calculator functions correctly and efficiently. The minimum requirements are hardware and software dependent, and are outlined below.

Hardware

- Intel Architecture Pentium 4 or equivalent
- 512 MB Ram
- 100 MB disk space

Software
Either one of these operating systems can be used.

- Microsoft Windows 2000 Professional – Server Service Pack 3
- Microsoft Windows XP Professional – Service Pack 1

STV calculator comparisons

There are significant differences in the performance and the installation requirements of the two certified STV calculators.

Backup calculator

- Requires a SQL Server database to store data and calculate results.

- Is much slower at loading data and calculating results than the main calculator
- If this calculator is used, several calculators on different PCs may be required to calculate a preliminary result at close of voting.

Main calculator

- Doesn’t require its own SQL Server database; all data is held in the PC’s RAM.
- Much faster than the backup calculator.
- Most local elections can be calculated on a single fast PC within a reasonable timeframe after close of voting.

While the main calculator is impressively fast and only one PC may be needed to calculate STV results, it would be prudent to have more than one PC available for this task at close of voting.

Organisation for intermediate files

The STV calculator has been designed to derive the name of its XML-encoded output file from the name of its input file, and to create the output file in the same file-system folder as the input file.

Good practice requires that there be created, in the server’s disk filing system, an organisation of folders that clearly separates the intermediate XML-encoded files that contain preliminary and final result data.

The logical organisation of folders will partly depend upon the personal preference of the EO, provided that the organisation the EO chooses helps reduce to a minimum the chance of a wrong file being selected by an operator.

Where an operator is required by the software to choose the name of an intermediate file, there needs to be rules to assist the operator to compose each filename. In particular, filenames should indicate:

- whether the file contains data or results that are preliminary or final;
- the date and time that the data was extracted from the recording database.

Use of the backup STV calculator

The backup STV calculator is intended for use only when the main calculator cannot produce a result. If a problem arises, you should follow this very brief preliminary check-list.

- Problem with other software
  The STV calculator counts votes only when it receives the data input file. Any problems before that point do not involve the calculator.
- STV calculator does not start
  Check that the calculator has received the data input file. The calculator cannot start the count until it receives the input file.
- STV calculator produces error message
  Analyse the error message and take appropriate action as per the calculator documentation.
- Problem not resolved and calculator does not produce result.
  Use the backup STV calculator.

It is important to note that the two calculators have different requirements. The backup calculator does not include some of the features that make the main calculator easy to use. It is not expected that any EOs will need to use the backup calculator. However, it should be available on at least one PC to use if required.

DIA recommends that the backup (IPL Ltd) calculator is installed on a separate computer to the main (CGNZ Ltd) calculator.

Barcodes on voting documents

Use of check characters

When printed barcodes are used on voting documents, the barcodes should contain check characters to reduce the likelihood of data input errors.

The electoral roll

Roll versions

Leading up to an election, three versions of the electoral roll are normally supplied to an EO by the Electoral Enrolment Centre. The first is for software testing, the second is the "Checkit" or preliminary roll and the third is the final roll.

Make sure that the printed rolls are produced from the correct database versions, and that the voting documents are produced from the final roll data. The EO must have sufficient checks for knowing which version of the electoral roll is loaded into the database at any stage.

Each roll is supplied with an accompanying text file or printout listing the number of electors in each ward, the number of "194" records and the total number of elector records supplied. Taken together with known numbers of merged ratepayer electors, these numbers can be cross-checked against the entries on the printed ward rolls and against the number of entries on each ward extract file from the database that drives the voting documents paper printing process.

Make sure that all media supplied by the Electoral Enrolment Centre is clearly labelled and stored securely.

Use of the electoral roll data

The electoral roll is compiled from data collected for the sole purpose of running elections. The principles contained within the *Privacy Act 1993* limit the use of the electronic electoral roll data to the purpose for which it has been collected; that is, to the running of an election.

The Electoral Enrolment Centre, the agency that has collected the data directly from individuals, supplies the electoral roll to EOs to run their elections and for no other purposes. EOs and their IT staff need to be aware of this and to ensure that the electronic electoral roll is not copied or redistributed to any other person for any other purpose.

Keeping the Master Roll

Regulations 69(1) and *114((1)* require the EO to retain copies of the final or master roll, as used for the scrutiny, until the next triennial election. Furthermore, the roll must be available for inspection by an elector in the same local government area.

It would be wise to keep the electoral roll on the medium originally supplied by the Electoral Enrolment Centre together with the printable electronic files (including ratepayer electors) derived from it, in case the EO wishes to reprint a roll at any time.

It is clearly a legitimate use, under the regulations, of the electoral roll for an electronic copy to be maintained until the following election on the council’s computer network and accessible by a simple enquiry program, to assist enquiries from electors.

Voting document processing procedures

Definitions

The *LER* uses the following terms in respect of FPP and STV elections, particularly where computer systems are used to process the voting documents

FIRST PAST THE POST (FPP)	SINGLE TRANSFERABLE VOTE (STV)
”**Checking system** means a system that: (a) is designed to ensure that (i) votes recorded from valid voting documents correctly record the intentions of the voters expressed in those voting documents, and (ii) votes are counted correctly, and (iii) results are determined correctly according to the First Past the Post electoral system, and (b) may include components that (i) identify errors and processes likely to generate errors, including (but not limited to) components that entail the (A) repetition of operations and the comparison of the results produced without varying the processes used to perform the operation or by using different processes to perform the operation, and (B) use of selection methods, for example, selecting all operations or selecting operations by type or selecting operations carried over a period of time or selecting selection operations by sampling (ii) correct errors, (iii) modify processes so that they are less likely to generate errors; and (c) must, if practicable, correct any errors that it identifies.”	”**Checking system** means a system that: (a) is designed to ensure that preferences recorded from valid voting documents correctly record the intentions of the voters expressed in those voting documents; and (b) may include components that (i) identify errors and processes likely to generate errors, including (but not limited to) components that entail the (A) repetition of operations and the comparison of the results produced without varying the processes used to perform the operation or by using different processes to perform the operation; and (B) use of selection methods, for example, selecting all operations or selecting operations by type or selecting operations carried over a period of time or selecting selection operations by sampling: (ii) correct errors (iii) modify processes so that they are less likely to generate errors; and (c) must, if practicable, correct any errors that it identifies.”
“**Operation** with respect to a checking system, includes any act for the purposes of *regulations 56 to 58, 78 and 79* and any set of such acts, including (but not limited to) a set of acts defined by sampling.”	“**Operation** with respect to a checking system includes any act for the purposes of *regulations 101, 102 and 123*.”

“Process or **processing voting documents** means to carry out any process that facilitates the efficient counting of votes, and: (a) includes (i) opening returned envelopes (ii) extracting voting documents (iii) rejecting blank or informal voting documents (iv) identifying valid voting documents (v) recording votes from valid voting documents and putting them in a form for counting in an automated counting process; but (b) does not include counting votes.”	**“Process** or **processing voting documents** means to carry out any process that facilitates the efficient counting of preferences, and includes: (a) opening returned envelopes (b) extracting voting documents (c) rejecting blank or informal voting documents (d) identifying valid voting documents (e) recording votes from valid voting documents and putting them in a form for counting by a certified counting programme.”

Password testing

All passwords should be pre-tested to ensure they are functional on the day required. Where multiple passwords are required to access a system, passwords should be tested to the lowest level of access. The ability to reissue passwords on the day should be available along with the ability to release user profiles that have been locked from successive incorrect login attempts.

Counting votes

Regulations 58, 79, 103 and 123A require the EO to determine the preliminary result of the election (or poll) as soon as practicable after:
(a) all ordinary voting documents have been processed; and
(b) the close of voting.

The determination of the preliminary result:
(a) must be made using all ordinary votes; and
(b) may be made by also using special votes from valid special voting documents identified at that time

In addition these regulations also require the EO to determine the official result of the election (or poll) as soon as practicable after:
(a) all special voting documents have been dealt with under the regulations; and
(b) the scrutiny of the roll has been completed and disallowed votes dealt with.

This determination must be made using all votes.

Checking systems

Regulations 59, 79A, 104 and 124 require the electoral officer to apply a checking system to the processing and counting of votes.

Performance standards for checking systems are set out in *regulations 60, 79B, 104A and 124A*. The checking system must ensure that the results of the counting are at least as accurate as those that would be produced by:
(a) carrying out the following operations manually
(i) rejecting blank voting documents and informal voting documents;
(ii) counting votes from valid voting documents; and
(b) repeating the operations in paragraph (a); and
(c) resolving any discrepancies.

In determining whether or not the performance standard is met, it is sufficient to make reasonable inferences about the errors that are likely to be generated by the operation of the checking system.

Audit trails

Documentation of system and processes

Documentation of the system configuration, security measures and processes should be available for inspection by scrutineers.

Traceability

As a general rule, any important manual or partially manual steps need to be traceable. This will include such things as entry of data from batches of voting documents. It might also include any manual adjustments (adding specials) or reorganisation of results between the output from the computer system and publishing of results.

If special votes are added manually into the results of an FPP election, copies of the unedited and edited results documents should be kept so that the editing process remains evident.

The entry of batch data into the computer system needs to be manually logged with date, time and operator information on batch recording sheets.

Checks for completeness

The EO needs to ensure that processes are in place and reports available from the application software to ensure that all voting documents received are fully processed.

Miscellaneous

Understand your software!

Regulation 91(2) states that any regulation (from the STV part of the regulations) which refers to a determination or any other action of an EO also includes an action taken by an automated process. So, you need to be aware of exactly what your computer software is doing and be responsible for it!

This explicit requirement is not included in the FPP regulations, although, clearly, good practice requires you to understand your software as best you can under all circumstances.

Building electricity supply

Have an electrician check the adequacy of the mains power to the election office, sufficient to run all the equipment with a suitable margin of reserve. Be aware that if you start-up all the equipment at the same time, you may overload the supply and lose power. You may need to upgrade the power supply to the election office, or provide additional power outlets for the computers, printers and other equipment. Before this can be done, you will need a plan of the proposed layout for all your PCs, printers and other electrical equipment.

Electrician

Have an electrician on call at all times when you cannot afford to lose mains power.

Service Level Agreement

Everything that your IT support organisation promises to do for you should be documented and signed off. A council's IT department will be able to offer you their standard service level agreement (SLA), which you should extend as required. Also ensure SLAs and response plans from all main suppliers (such as the election software supplier) are documented and signed.

Systems/Network Engineer

Ensure that there is a Systems/Network Engineer available for the duration of the election, espe cially when you cannot afford the network to be unavailable for an extended period. Ensure that you have all appropriate methods of contact (e.g. mobile, pager, home number) or that the engineer is on site for the required period. Similarly, organise the availability of an engineer who can fix your server and recover your database at short notice. Ensure that the engineer is familiar with your election database and its configuration. Make sure that all relevant installation and configuration parameters and processes are documented in case the database needs to be recreated on a new server at short notice.

Server and network availability

Insist that there are no planned maintenance outages or upgrades on any component of your system, for the period of the election. This must include down-time for air-conditioning systems, or after-hours testing of backup power generators that might affect the server or the network.

Uninterruptible power supply unit (UPS)

An uninterruptible power supply unit (UPS) may be worth installing to protect all or part of your system from power fluctuations and also to allow sufficient time for a controlled shutdown should a mains power failure occur. It is particularly important to secure the database server against external disruptions. Ideally backup the UPS with a standby generator to allow continuous operation in the event of a mains power failure.

Fire prevention

Adopt a policy of turning off the power to all electrical equipment (except, perhaps, the database server) in the election office during times that the office is not occupied.

Spare Equipment

Decide how many spare PCs and printers you need, and ensure that they are configured ready to use without delay if an equipment failure should occur. If your operation depends on a network link to another building, make sure that suitable network equipment is available.

Provision for judicial recount

When hiring equipment, allow for the possibility that you may need to retain some of the equipment for a judicial recount.

Data removal

Where any computer has been hired for use in the election, ensure that all software and data has been permanently removed from storage devices before the equipment is returned to the leasing company. Use the US DOD standard 5220.22-M with 7 over-write passes as a minimum standard for secure wiping.

Workplace safety policy

You must have a workplace safety policy and it must include factors relating to the correct use of computers and the provision of satisfactory conditions for computer operators.

There are currently two important documents published by the Occupational Safety and Health Service of the Department of Labour, New Zealand. www.dol.govt.nz
These are:
"Visual Display Unit Safely – How to use your"
http://www.osh.dol.govt.nz/order/catalogue/262.shtml

"Visual Display Units in the Place of Work – Approved Code of Practice for the Safe Use of"
http://www.osh.dol.govt.nz/order/catalogue/220.shtml

Both these documents can be downloaded as PDF files.

GLOSSARY

Abbreviations

EO	Electoral Officer
IPL	Information Power Ltd, created the first STV calculator. Now called the "backup" calculator
CGNZ	CAP Gemini NZ Ltd, created the second STV calculator. Now called the "main" calculator
EEC	Electoral Enrolment Centre
IT	Information Technology
DIA	Department of Internal Affairs
FPP	First Past the Post electoral system
STV	Single Transferable Voting electoral system
USB	Universal Serial Bus, a type of computer interface connection.
SLA	Service Level Agreement
DHB	District Health Board
UPS	Uninterruptible Power Supply

Use of the terms 'random' and 'pseudo-random'

Regulation 31(5) defines the terms, pseudo-random order and random order as follows:

- Pseudo-random order means an arrangement where:
  (a) the order of the names of the candidates is determined randomly; and
  (b) all voting documents use that order.
- Random order means an arrangement where the order of the names of the candidates is determined randomly or nearly randomly for each voting document by, for example, the process used to print each voting document.

FINALLY

If, in spite of all this good advice, your computer network turns to custard and ruins your election, this may help you feel better as you collect your final pay-cheque.

Why computers sometimes crash!

If a packet hits a pocket on a socket on a port,
and the bus is interrupted as a very last resort,
and the access of the memory makes your floppy disk abort,
then the socket packet pocket has an error to report.

If your cursor finds a menu item followed by a dash,
and the double-clicking icon puts your window in the trash,
and your data is corrupted 'cause the index doesn't hash,
then your situation's hopeless and your system's gonna crash!

If the label on the cable on the table at your house,
says the network is connected to the button on your mouse,
but your packets want to tunnel to another protocol,
that's repeatedly rejected by the printer down the hall...

And your screen is all distorted by the side-effects of gauss,
so your icons in the window are as wavy as a souse,
then you may as well reboot, and go out with a bang,
'cause as sure as I'm a poet, soon the sucker's going to hang.

When the copy on your floppy's getting sloppy in the disk,
and the macro code instruction's causing uninvited risk,
then you'll have to flash the memory and you'll want to RAM your ROM,
and then quickly cut the power, lest it goes off like a bomb!

(With apologies to Dr Seuss!)

SOLGM
NEW ZEALAND SOCIETY OF
LOCAL GOVERNMENT MANAGERS

PART 15: APPENDIX C THE STV CALCULATORS – TIPS AND TRICKS

CONTENTS

INTRODUCTION

This document covers aspects of use of the STV calculator relating, in particular, to the prevention of errors and actions to be taken should they occur. Some of the information assembled in this document has come from other sources. You should carefully read all other documents, especially those provided with the STV calculator and others that might be found on the www.stv.govt.nz web site.

The abbreviations CGNZ refer to Cap Gemini NZ Ltd, who wrote the main STV calculator.

The abbreviation IPL refers to Information Power Ltd, who wrote the backup STV calculator.

In some sections of this document, information is directed separately at electoral officers or their IT support. In other cases, information applies to both. This has led to the table-based organisation of this document.

The most important steps in dealing with errors from or involving use of the STV calculator is to identify the type of error and what is, in general terms, causing it. Beyond that, the processes for dealing with the errors are so potentially diverse that it is impossible to document them all in detail. What you must ultimately do is, together with your IT support, take what steps are required, based on a thorough understanding of the requirements of the STV calculator and a detailed knowledge of PC technology.

At a technical level, leave it to your IT support to sort out. If you need to call a help line, be very clear which source of help you need to call.

We hope you find this document useful!

YOUR SOURCES OF HELP

Your organisation's IT help desk

It is absolutely vital that your election team contains at least one person with IT expertise. Having that person around when things go wrong will be a big help to you.

Your software provider

Your application software provider will know everything that needs to be known about the integration of both STV calculators into their package. You will need their help if the STV calculator appears to break, because there is a high probability that the problem will be caused by an input data fault.

PREPARING THE MAIN STV CALCULATOR FOR USE

Make sure that the main STV calculator is installed on a PC that has not previously had the backup STV calculator installed. This can lead to issues. You are advised to start with a freshly configured PC.

SIZING THE PC

Electoral officers	IT support
Make sure that each of the PCs to be setup to run the STV calculator are sized according to the recommendations of both CGNZ and IPL. The CGNZ specification is the more demanding of the two.	From the main STV calculator Software Installation Guide[1] **Hardware** • Intel Architecture Pentium 4 or equivalent • 512 MB Ram • 100 MB Disk Space **Software** Either one of these operating systems can be used: • Microsoft Windows 2000 Professional or Server – Server Service Pack 3 • Microsoft Windows XP Professional – Service Pack 1

CORRECT INSTALLATION

Electoral officers	IT support
The STV calculator uses Microsoft's XML parser to do much of the XML-encoded text handling. Make sure that earlier versions of this product are removed from the PCs before installing the STV calculator.	**MSXML component** Please ensure that any previous version of MSXML components are un-installed before installing the STV calculator. MSXML refers to the Microsoft XML Parser, which the STV calculator uses to parser all the XML-encoded text read from the input and configuration files. The "previous version" referred to above is any version earlier than version four. If you already have version four (or later) installed, you can leave it installed. Otherwise use the *Add/Remove Programs* control panel to uninstall the XML Parser before installing the STV calculator. If you allow the installation wizard to use the default locations, you will see the *C:\Program Files\STVCalculator* folder and its subfolders created. But note that the *VerificationTestFiles* folder is not automatically copied from the CDROM. Note also that you need to have local administration rights to the PC to do the installation. If you do the installation using a login name different to the name to be used to run the STV calculator, you will need to ensure that you tell the installation wizard to install the product for "*Anyone who uses this computer*" when in the appropriate wizard window.

[1] Software Installation Guide, August 2003, CGNZ Ltd. Available from the installation CDROM

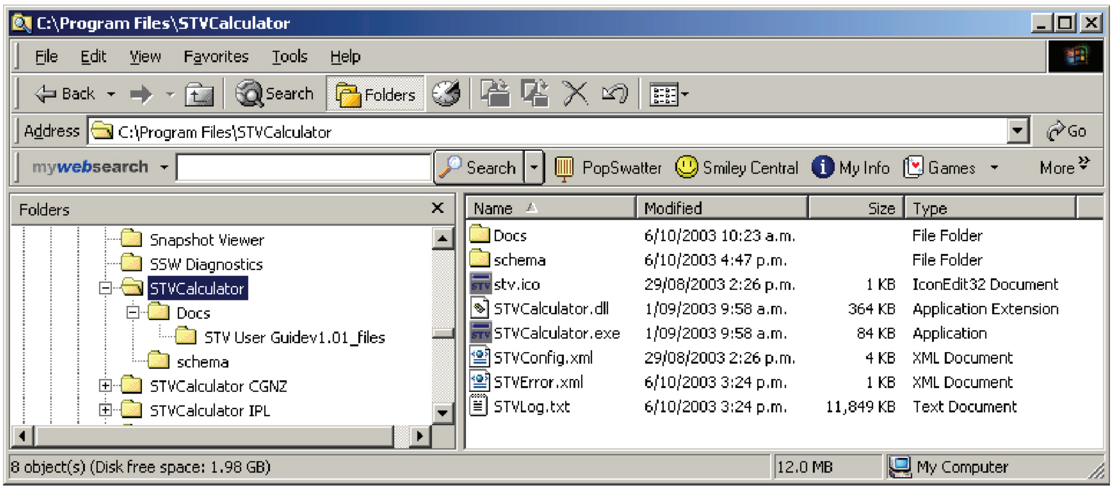
Please be aware that when the STV calculators were developed, the latest version of Windows XP was Service Pack 1 (SP1). Later service packs have been released for Windows XP, and you can confidently expect that the STV calculators will continue to run under these later service packs.

However the Microsoft XML Parser (MSXML) is a critical component of the STV calculators and MSXML version 4 was used in the STV calculator development. Later releases of MSXML have subsequently appeared, and version 6 is shipped with Microsoft SQL Server 2005, Visual Studio 2005, NET Framework 3.0, Windows Vista and Windows XP Service Pack 3. It also has support for native 64-bit environments. It is an upgrade but not replacement for versions 3 and 4 as they still provide legacy features not supported in version 6. Versions 6, 4 and 3 may all be installed and running concurrently.

It is important, therefore, to ensure that MSXML version 4 is installed on all PCs that will run the STV calculators. Microsoft also state that the latest release of version 4 is MSXML 4.0 SP3, released in March 2009. Microsoft's support for MSXML 4 expires in November 2009.

What the main STV calculator installation gives you

The installation process places the components of the STV calculator as illustrated below.



C:\Program Files\STVCalculator

Address C:\Program Files\STVCalculator

- Snapshot Viewer
- SSW Diagnostics
- STVCalculator
  - Docs
    - STV User Guidev1.01_files
  - schema
- STVCalculator CGNZ
- STVCalculator IPL

Name	Modified	Size	Type
Docs	6/10/2003 10:23 a.m.		File Folder
schema	6/10/2003 4:47 p.m.		File Folder
stv.ico	29/08/2003 2:26 p.m.	1 KB	IconEdit32 Document
STVCalculator.dll	1/09/2003 9:58 a.m.	364 KB	Application Extension
STVCalculator.exe	1/09/2003 9:58 a.m.	84 KB	Application
STVConfig.xml	29/08/2003 2:26 p.m.	4 KB	XML Document
STVError.xml	6/10/2003 3:24 p.m.	1 KB	XML Document
STVLog.txt	6/10/2003 3:24 p.m.	11,849 KB	Text Document

8 object(s) (Disk free space: 1.98 GB) 12.0 MB

<table>
<tr><th colspan="2">VERIFICATION TESTS</th></tr>
<tr><td><b>Electoral officers</b></td><td><b>IT support</b></td></tr>
<tr><td>By comparing the output of the STV calculator to the supplied output files, you can be certain that the STV calculator is working and giving the correct result. However, the supplied verification files contain only small amounts of test data, so you may want to perform additional testing using the test data previously supplied with the backup STVcalculator.</td><td>When the installation is finished, copy the <i>VerificationTestFiles</i> folder from the CDROM to the PC's hard disk and follow the instructions in the installation guide.</td></tr>
<tr><th colspan="2">LOAD TESTS</th></tr>
<tr><td><b>Electoral officers</b></td><td><b>IT support</b></td></tr>
<tr><td>Running all the scenarios from this group of test datasets will give you confidence that the PC is adequately configured and correctly installed.</td><td>The test data previously supplied with the backup STV calculator enables you to do some more realistic load testing. In particular, scenario 6 provides data from 999,990 voters. This data can take about 20 minutes to load and validate, but reaches a result quickly after only three iterations.</td></tr>
</table>

SIGNATURE CALCULATION TOOLS

Electoral officers	**IT support**
There is some value in using the *Secure Hash Algorithm 1* (SHA1) signature verification feature built into the STV calculator. You can use it to check whether or not any file (a data file or the STV calculator itself) has been unexpectedly modified.	The tools you will need to manually calculate a signature can be downloaded free from www.slavasoft.com. *HashCalc* is the version with a graphical user interface, while *Fsum* has a command line interface and can be bound into other software. The way it works is as follows. • An input file for the STV calculator is created by your election software. • The SHA1 software reads the file and calculates a 40-character signature. This is stored in another text file. • The input file is eventually read by the STV calculator and, if signature-checking is required (it's optional), the STV calculator computes the SHA1 signature of what it reads. • The STV calculator is also passed the name of the file that holds the original SHA1 signature. It compares this with what it has calculated. • If the signatures match, the STV calculator proceeds. Otherwise it raises an error to the operator. • If it proceeds, the STV calculator will also calculate and store a SHA1 signature for the output file. The use of SHA1 signatures with STV calculator input files is optional, but it can be used to provide a further layer of security around input and output files for the STV calculator. But be aware that is not practical to calculate signatures manually for all of the STV calculator input files. Your software provider must build this into the part of the package that creates input files for the STV calculator. Furthermore, you can, at any time, use the *HashCalc* tool to check that the calculator itself has not been corrupted by a problem with the PC's Windows filing system. To do this, you should first calculate the SHA1 signatures for the two files *STVCalculator.dll* and *STVCalculator.exe* from the installation CDROM. Copy and paste the two signatures into a text file and save it on the PC. At any later stage, you can use *HashCalc* to calculate the SHA1 signatures for the same two files from their location on the PC in *C:\Program Files\STVCalculator*. If the signature matches the stored values, you can be absolutely sure that the STV calculator program is unchanged. The same principle applies to any file at all. You can calculate an original signature and verify that it has not changed later. It is important to note that the SHA1 calculation is done in a intelligent way and the act of accessing a file does not, by itself, change the signature. For example, the "Last accessed" file property is not included in the signature calculation. Also, you can do things like lock the file to *read-only* without changing the signature. But you cannot change the data or any executable code in the file without it resulting in the SHA1 signature being altered. In the calculator's *Software Installation Guide*, under *Cryptographic Verification*, it is stated that the SHA1 signatures for the STV calculator will be published on the Web. At the time of writing, this has not happened. Nor is there any mention of this on the STV calculator installation CDROM, as expected.

QUARANTINING	
Electoral officers	**IT support**
It is absolutely vital that, once the installation and testing on the STV calculator PCs is finished, they are secured from any further changes. You may wish to keep them in a locked room. You need to be sure that when you come to calculate your election results, they will not fail because someone has changed or deleted an important component.	If you need to make any changes to the software or any other aspect of the STV calculator PCs, make sure you run all the previously used tests and log what you have done for later reference.

THE GRAPHICAL USER INTERFACE (MAIN STV CALCULATOR)

There are two ways that the main STV calculator runs.

- While bound into an election software package. In this case the STV calculator is under control of the package and you do not interact directly with it.
- Under your manual control. You enter its parameters and it tells you what it is doing.

When running the STV calculator manually (through the graphical user interface), there are fields to complete to tell the STV calculator from where to get its input data and where to place the output data. There are also fields relating to the signature files if required.

Try to use the buttons to the right of the fields and browse to files or folders that you require in the fields. It is too easy to type an incorrect file path and not notice the mistake.

You may find the graphical user interface frustrating in some respects. The available space in the fields above may not be sufficient to display a complete path name. However, you can click into a field and arrow to the right or left as you need.

Also, the STV calculator does not remember what you previously entered when you next run it. So, you might choose to leave the STV calculator in memory between calculations.

RESOLVING PROBLEMS – GENERAL ADVICE

DOCUMENT WHAT YOU DO
Besides the obvious stuff like "be logical" and "consult your IT support", the most important thing you need to do is *document* each problem and your resolution steps. Record the error message by copying and pasting (alt-Print Screen) the message window into Word or WordPad as a record that you can perhaps email to a help desk if required. You can also copy and paste the STV calculator GUI window into the document as a record of the input and output files you selected. You should also keep a detailed record of what you were asking the STV calculator to do, together with the steps you took to isolate the problem.

CLASSIFY THE PROBLEM

Browsing through the list of error codes and their description in the Troubleshooting section of the User Guide[1] is highly recommended. All the errors that the STV calculator has been programmed to detect are described there. Any that are unexpected are very unlikely to occur. None have been reported while the STV calculator has been used in real elections.

Errors fall into the following broad categories. When you see an error being reported, sort out in your own mind what type of error condition it is. The help you call for, if you can't fix the problem yourself, will depend on the error class.
Depending on how IT-literate you are, you may choose to have an IT specialist help you interpret any error reported by the STV calculator. This is highly recommended!

CHECK THAT THE PROBLEM IS REPEATABLE

Try it again to see if you get the same error with exactly the same symptoms. This step is important because it usually eliminates random operator mistakes like a typing mistake, or selecting the wrong input file. Sometimes inconsistent symptoms will suggest a hardware problem with the PC.

[1] Software User Guide, August 2003, CGNZ Ltd. Available from the installation CDROM

RESOLVING PROBLEMS – SPECIFIC ADVICE

THE STV CALCULATOR DOES NOT START

Check that the STV calculator has received the data input file. The STV calculator cannot start the count until it receives the input file.

PROBLEMS WITH OTHER SOFTWARE

Electoral officers	**IT support**
The STV calculator counts votes only when it receives the data input file. Any problems before that point do not involve the STV calculator.	If you cannot find the output that you expected, look at C:\Program_Files\STVCalculator\STVError.xml This file records the last error that the STV calculator raised. The STV calculator overwrites this file every time it raises an error. C:\Program_Files\STVCalculator\STVLog.txt This file is a cumulative log of everything the STV calculator has done. It may take a while for a text editor, such as Notepad, to open it. Go to the end of the file and scroll back to see what the last calculation was.

STV CALCULATOR PRODUCES AN ERROR MESSAGE

Analyse the message and take appropriate action as described in the User Guide. All known errors are listed in the User Guide. Look for the error message and, if you find it, follow the instructions. If you do not understand the instructions, ask your IT specialist for assistance.

PC CONFIGURATION ERRORS

Electoral officers	**IT support**
There will be an error message that looks decidedly "technical" and isn't one of those documented in the STV calculator Users' Guide. Refer the problem to your IT specialist.	The PC might be missing the Microsoft XML Parser or some other operating system component that the STV calculator depends upon. You will most probably recognise such situations and arrange to either reinstall the STV calculator or the missing operating system component.

FILE SYSTEM ERRORS

Electoral officers	**IT support**
This includes simple problems like the PC filling its hard disk. You should never let your hard disks get more than 90% full (this is not a critical figure, but a useful target!). Errors when reading from and writing to a hard disk are sometimes hard to recognise and may not be fixable in a short enough time-frame. For this reason, you should setup more than one PC to do your STV calculations.	If the PC's disk is full find out what has filled it. A utility like "TreeSize Pro" is ideal for this, as it quickly finds out and displays the size of each folder and file on the nominated storage device. Keep in mind that, with a default installation and the default operating parameters set, the STV calculator is logging its work to *C:\Program Files\STVCalculator\STVLog.txt*. This is in addition to the output files that you are, of course, aware of. Keep a watch on this file and make sure that you are always operating with plenty of free disk space in reserve.

STV CALCULATOR INSTALLATION ERRORS

Electoral officers	**IT support**
To run correctly, the STV calculator depends upon a configuration file and twelve schema definition files. These are all written into the same folder that contains the STV calculator, at installation time. In this situation, reinstalling the STV calculator (using the recommended default locations) will correct the problem. Your IT support staff can do this for you if required.	If you change or delete any of these files, the STV calculator will probably not run. When you install the STV calculator, you should make a note of the names and locations of these critical files so that you can quickly check later if a problem arises. The STV calculator will report if any of these files are missing or contain data that is meaningless to it.

<table>
<tr><th colspan="2">INPUT DATA ERRORS</th></tr>
<tr><td><b>Electoral officers</b></td><td><b>IT support</b></td></tr>
<tr><td>These errors occur when the STV calculator decides that some input data is missing from the set of input files presented to it.
It may be that one or more files out of a set of input files for one election issue have been accidentally deleted or incorrectly generated by the application software.</td><td>If the STV calculator reports missing input data files or a data inconsistency, you will need to contact the supplier of your election software.
Looking at the data structures contained by the test datasets will clearly indicate the role of each file and how they are supposed to be linked together. You may be able to spot the problem by opening the master input file and looking at its contents, especially the links to the files containing voters' preferences.</td></tr>
<tr><th colspan="2">USER ACTION ERRORS</th></tr>
<tr><td><b>Electoral officers</b></td><td><b>IT support</b></td></tr>
<tr><td>There is only one user action that will raise an error. This is when the user clicks on the CANCEL button on the interface during the data loading or before the calculation is completed. Clearly, this is a situation that the user will recognise and no further assistance is required.</td><td></td></tr>
<tr><th colspan="2">PROBLEM NOT RESOLVED AND STV CALCULATOR DOES NOT PRODUCE RESULT</th></tr>
<tr><td colspan="2">If you and your IT expert cannot find the error documented in the User Guide, and you cannot otherwise make sense of the message, or if the message suggests a STV calculator fault condition over which you have no control, then use the backup STV calculator.
At what point you decide to try running the backup STV calculator with the <i>same input data</i> is ultimately your own decision. However, you should be certain that you have taken every possible step to identify operator error and input data error before you come to the unfortunate conclusion that the STV calculator "contains a bug".
Clearly, if you decide to use the backup STV calculator and it also fails to produce a result with the same input data, then the problem lies with your input data, your PC, or the way you are using it. Remember that if you are running the main STV calculator with SHA1 digital signatures, you will need to regenerate the input files without signatures. In this event, you would expect the regenerated files to contain exactly the same input data for the STV calculator.</td></tr>
</table>

THE BACKUP STV CALCULATOR

The backup STV calculator is different!

1. Requires a SQL Server database to store data and calculate results. This is setup automatically when you install it.

2. Is much slower at loading data and calculating results than the main STV calculator. For this reason, you should avoid using it for other than emergencies.

3. If this STV calculator is used, several calculators on different PCs may be required to calculate a result at close of voting within your required time-frame.

4. The graphical user interface for the backup STV calculator is different to that of the main STV calculator.

5. It doesn't support the use of SHA1 digital signatures, so your input files will need to be created without associated signature files.

Your software supplier will need to have made provision in the design of the supplied election software package for the input files to be compatible with both the main and the backup STV calculators. Depending on aspects like SHA1 signatures, you may have to regenerate the STV calculator input files before using the backup STV calculator.

Preparing the backup STV calculator

In the very unlikely event that you have an issue with the main STV calculator, and decide to use the backup STV calculator, you will not want to spend time configuring and testing it just at that time. So make sure that you have the backup STV calculator already installed, testing and waiting on another PC. And make sure you have practised using it so if the need arises, you know exactly what to do.

When to use the backup STV calculator

The backup STV calculator is intended for use only when the main STV calculator cannot produce a result. How you go about this depends largely on a process that your software supplier recommends. Whatever the method, you should have practised using the backup STV calculator on the supplied test scenarios well in advance, and you should have available procedural documentation from your software supplier, or which you have written yourself with help from your IT support people.

SOLGM
NEW ZEALAND SOCIETY OF
LOCAL GOVERNMENT MANAGERS

PART 15: APPENDIX D VOTE PROCESSING AND COUNTING ASSURANCE

GUIDELINES FOR ACHIEVING ASSURANCE ON VOTE PROCESSING AND COUNTING IN LOCAL ELECTIONS AND POLLS

CONTENTS

PURPOSE OF THIS DOCUMENT

This document addresses particular election management issues arising from the inquiry into the 2004 local authority elections conducted by the Justice and Electoral Committee (JEC). These issues fall into the category of vote processing and counting.

In response to the JEC's report, the SOLGM Electoral Working Party (EWP) has developed these guidelines to provide a framework for '*end-to-end' assurance* on the sequence of vote processing and counting stages in New Zealand local authority elections and polls.

The objective of the EWP, in producing these guidelines, is to assist electoral officers to meet the expectations of both their local authority and the public that local elections and polls are conducted in a manner that produces accurate and timely results. This applies whether the election or poll is conducted in-house by the electoral officer or is contracted to an election service provider.

To help achieve this objective, the EWP recommends that the electoral officer satisfies him or herself that the information technology tools and business processes used in any election or poll are well documented, independently tested and *fit for purpose*.

ISSUES ADDRESSED

These guidelines address, wholly or in part, the following recommendations by the JEC:

> Further consideration be given to the most appropriate method of providing the required assurance around vote processing and counting systems including the need/practicality of *'end-to-end'* certification.

Much of these guidelines are concerned with determining the fitness for purpose of software components and business processes to achieve '*end-to-end' assurance*. This is recommended as an alternative to certification.

> A complete *'end-to-end'* counting process should be formally documented.

These guidelines address this issue on two levels. Firstly, they provide a breakdown of typical *'end-to-end'* counting processes for both first past the post (FPP) and single transferable voting (STV) elections. Definition of an '*end-to-end' assurance* counting process is necessarily generic. The detail in the process depends upon the software system used to implement the steps in that process and also upon the business processes adopted by the electoral officer. The reason for including the generic descriptions is to ensure both electoral officers and other interested parties understand the nature and elements of the '*end-to-end' assurance* counting process.

Secondly, it is essential for electoral officers that their particular '*end-to-end' assurance* system is documented in appropriate detail. This includes documentation for any software package provided to them to ensure the package is correctly used. There must also be documentation of (essentially manual) steps that are not implemented by software components and their associated controls.

> Electoral officers should have a good understanding of the contractor's approach, understand the key steps and controls within that approach, and consider the need, nature and extent of pre-count verification of the system and controls.

These guidelines strongly support this recommendation. The electoral officer remains accountable for the proper conduct of an election or poll whether or not all or part of the election process is contracted out. To assist the electoral officer to have confidence in the electoral outcomes, the electoral officer needs to have a full understanding of any contractor's systems and processes. A recommendation relating to the appointment of an independent auditor is designed to help achieve the required confidence.

> **All parties should adhere to applicable codes of "best practice" for developing and operating in an information systems environment.**

The EWP strongly recommends the adoption of these good practice guidelines by electoral officers and other parties involved in the conduct of local elections.

DEFINITIONS

Assurance

These guidelines use assurance in its general meaning of seeking to ensure or make certain of a particular outcome. In the context of local authority elections and polls, this outcome is the production of accurate and timely results. The outcome relates to both business processes and information systems employed at a particular election or poll and is achieved through independent testing of processes and systems, and full documentation including training material, reports and business process definitions to support the successful outcome of the election.

Audit

These guidelines use the term *audit* to mean the subjecting of all information technology (IT) applications and all automated and manual procedures to independent examination to confirm that they have been defined and implemented appropriately to perform their required tasks without error or to enable identification of any error or fault should it may occur. Appropriate levels of sample testing are required to support an audit report. An *audit* would not normally involve the detailed examination of software components, but rather provide an assurance that all software components have been independently tested within the defined limits in which they are to be used.

Certification

These guidelines use the term *certification* to mean the subjecting of a component of a software package, or the whole package, to independent examination of the design of the package together with exhaustive testing to confirm desirable behaviour and identify any abnormal behaviour or unexpected faults in any environment. *Certification* requires absolute levels of evidence typically through full-scale 100 percent sample testing. It would normally be undertaken by a company with expertise in testing software systems. *Certification* is often used in a broader audit sense, but its use in these guidelines is restricted to the narrower meaning identified here.

Election or poll

Any reference in this document to an *election* is also intended to include a *poll* unless the context precludes it. *Elections* and *polls* cover both FPP and STV.

'End-to-end'

The EWP has, for the purpose of identifying boundaries for vote processing and counting assurance, defined '*end-to-end*' as being from the receipt of voting documents from voters to the production of election results. The generic steps involved in '*end-to-end*' processing and counting for both FPP and STV elections are set out in Attachment 1.

'Fit for purpose'

'Fit for purpose' is an expression that is used to describe the basic expectations of a business process or information system solution and its appropriateness for an organisation.

To be fit for the purpose of running a local authority election in New Zealand, the business processes adopted by an electoral officer, or a service provider, must meet legislative requirements, and should meet any code of practice or other mechanism for electoral guidance. Other industry expectations and generally accepted good practice should also be considered when determining the fitness for purpose of electoral processes.

In respect of information systems, either provided by a vendor or developed in-house, '*fit for purpose'* means that the IT system supporting the business processes is precisely appropriate for the purposes intended. For local authority elections, the system must be able to capture and process voting documents in accordance with process requirements. It must also provide adequate system controls to maintain voting document integrity and provide sufficient information to support the electoral officer in discharging his/her electoral duties.

Assurance on an IT system can be obtained either through independent certification of the software or by reliance on independently supervised testing that the system is '*fit for purpose'* in the particular environment in which it is to be used. In the context of local authority elections in New Zealand, the EWP believes it is appropriate to rely on '*fit for purpose'* testing of the system in a particular environment.

System

Wherever used in these guidelines, the word *system* is used in a general sense, not in reference to a specific piece or a package of software. A *system* includes the software and associated processes. The business processes that take returned voting documents right through to the results of an election are necessary parts of the electoral *system*.

DEALING WITH SPLIT RESPONSIBILITIES

These guidelines make no specific distinction between an election conducted completely in-house by an electoral officer and one conducted completely or in part by an election service provider. Each electoral officer will need to consider the application of these guidelines and in particular, detailed documentation to reflect the actual arrangements for his/her election.

For example, the required scrutiny may be performed by an electoral officer who subsequently transfers batches of voting documents to an election service provider for processing. In such a case, it will be necessary for the service provider to establish processes and control points that enable reconciliation of the voting documents across the electoral officer – service provider boundary.

Another circumstance to be addressed is where an electoral officer or service provider processes some voting documents and then transfers this data electronically to another electoral officer or service provider for completion of the processing and counting for the issue concerned.

In general terms, partial processing at different locations require special control points and reconciliation to provide assurance that voting documents are not lost or overlooked. In this type of scenario, '*end-to-end*' reconciliation that encompasses all transfer boundaries becomes even more important.

CONTINGENCY PLANNING

These guidelines focus on normal vote processing and counting processes within the '*end-to-end*' system as defined above. The assurance steps identified in these guidelines are designed to ensure this can proceed smoothly and to mitigate risks of problems in vote processing. All risks, however, cannot be entirely eliminated and electoral officers still require appropriate contingency planning and disaster recovery plans.

Part 15 of The Code of Good Practice for the Management of Local Authority Elections and Polls gives examples of the things that can go wrong at election time and the need for good risk management strategies to address these. The EWP strongly recommends that electoral officers, in association with any election service provider, develop such strategies in addition to adopting these guidelines.

ASSURANCE: INFORMATION TECHNOLOGY SYSTEMS

Assurance on IT systems can be sought at different levels.

Previous usage

An electoral officer may have had previous experience with an IT system and plan to use this substantially unchanged system again in the same way at the next election substantially unchanged. The EWP believes, even in these circumstances, that it is desirable for the electoral officer to be able to demonstrate to his or her local authority and, if necessary, the public that the system is '*fit for purpose*'. It believes the most effective way to achieve this is for the electoral officer to submit a '*fit for purpose*' certificate to the local authority. This certificate would be provided by an independent party (e.g. auditor) who has confirmed the system is able to capture and process all voting documents in accordance with documented rules, procedures and timeframes. The system documentation will also provide comfort that, in the event of the absence of the electoral officer, other less experienced persons can ensure that vote processing can continue unaffected.

'Fit for purpose' testing

If an electoral officer or his or her contracted service provider is using a new IT system or one that is substantially modified, then the electoral officer will need to be satisfied with the full range of functionality required to run the election. The EWP believes that the assistance of an experienced auditor is necessary to achieve this level of satisfaction. It is envisaged that the auditor and electoral officer would, among other things, agree on the nature and appropriate levels of system testing. The outcome must be that the system, and accompanying documentation, fully supports the running of the election and provides all the required controls to ensure accurate and timely election results in accordance with all statutory and good practice requirements.

Assurance would include:

- when the IT system is applied to the actual election, it will handle the full amount of data and run at a satisfactory speed to ensure timely and accurate election results;
- the IT system provides adequate system controls to maintain voting document integrity and provides sufficient information to support the electoral officer in discharging his/her electoral duties; and
- the processes that will be used to operate and support the IT system are appropriate, adequately documented and well understood.

Attachment 2 identifies detailed features expected to be included in '*fit for purpose*' software testing.

The EWP recommends that the auditor be requested to provide a '*fit for purpose*' certificate for the IT system to be used at the upcoming election and that the electoral officer submits a copy of this certificate to his/her local authority.

Independent certification

Certification goes beyond '*fit for purpose*' testing and proves the robustness of the IT system by more exhaustive testing including in a different (replica) environment. The certifier conducts full-scale tests on both desirable and abnormal behaviour of the system including testing with data containing faults. The certifier would verify all aspects of the system design as well as how the system handles unexpected events and usage. If the system includes complex algorithms, such as within the STV Calculator, certification provides sector assurance over a system function that may be costly to test individually.

Certification provides the highest level of system assurance. The EWP does not believe that this is necessary, as distinct from '*fit for purpose*' testing, and is unsure whether the necessary expertise is readily available to carry it out for the 2007 and subsequent local elections.

ASSURANCE: BUSINESS PROCESSES

Assurance on non-software manual business processes also needs to meet the'*fit for purpose*' test. This includes full documentation of these processes, procedures and training to ensure all electoral officials are fully conversant with the procedures they need to use.

The EWP believes that all electoral officers should consider the engagement of an independent auditor to provide assurance that the necessary business process documentation is in place. The focus of the professional audit assistance would be on all aspects of the electoral officer's *'end-to-end'* processes and systems that have not already been subject to independent testing. The final scope of the independent audit would be agreed between the electoral officer and the auditor. Attachment 3 addresses the recommended standard of audits.

Recommended good practice is that the electoral officer submits to his/her local authority a copy of the auditor's report on the *'end-to-end'* systems and processes to be used at the election.

RECOMMENDED GOOD PRACTICE

For the purpose of achieving assurance around *'end-to-end'* vote processing and counting at local authority elections, the EWP recommends the following good practice:

1. the electoral officer ensures he or she has a detailed understanding of the *'end-to-end'* vote processing and counting system that is to be used for the election(s) for which he or she is responsible including where responsibilities for vote processing may be split between different parties, and the system is fully documented;
2. the electoral officer uses, or contracts an election service provider to use, an IT system that has been proven to be *'fit for purpose'* as follows:
    a. if the IT system is supplied by a vendor or has been developed in-house, the electoral officer is provided with a certificate from an independent auditor confirming that the system has been tested and meets all the requirements for that election including being able to handle the required data volumes at the required speed;

    b. if the electoral officer contracts an election service provider to process and count votes, the electoral officer is provided with a certificate from an independent auditor confirming that the IT system to be used has been independently tested and meets all the requirements for that election including being able to handle the required data volumes at the required speed;
3. the electoral officer ensures all other vote processing and counting activities (outside the IT system) are fully documented and the appropriate electoral officials are properly trained and conversant with these business processes and procedures, and:

    EITHER

    a. for the purpose of ensuring these processes and procedures are *'fit for purpose'*, engage an independent auditor to provide a report for this purpose;

    OR

    b. adopt processes and procedures audited for another electoral officer;
4. the electoral officer submits to his or her local authority (for all territorial authorities, regional councils, district health boards and licensing trusts) a copy of the independent auditor's IT system *'fit for purpose'* certificate and business processes audit report along with confirmation of the particular IT system and business processes to be used at the upcoming election.

APPENDIX D: ATTACHMENT 1

VOTE PROCESSING AND COUNTING STEPS

In general, the steps defined below represent a continuous flow of manual and automated processes through which each batch of returned voting documents proceed. Most steps are simultaneously executing (on different batches) at any time during the vote processing stage of the election.

The CobiT control model

The EWP adopts the view, as described in detail in CobiT 4.0[1], that the existence and use of controls associated with all IT components and business processes is vital to the production of an accurate result.

CobiT 4.0 (pp 12-13) categorises IT resources into the following four groups:

- applications: the automated user systems and manual procedures that process the information;
- information: the data in all their forms input, processed and output by the information systems, in whatever form is used by the business;
- infrastructure: the technology and facilities (hardware, operating systems, database management systems, networking, multimedia etc, and the environment that houses and supports them) that enable the processing of the applications;
- people: the personnel required to plan, organise, acquire, implement, deliver, support, monitor and evaluate the information systems and services. They may be internal, outsourced or contracted as required.

While it is clear that each of the four groups of resources is vital to the successful outcome of an election or poll, it is the applications, together with their automated and manual procedures that need to be independently tested as *'fit for purpose'*.

As covered by CoBiT 4.0, the successful outcome of an election or poll relies on the information (voting documents), processed by the applications running on the infrastructure, operated by the people.

Translating this principle to an election system, we need definitive, measurable process control points to determine whether all voting documents, votes and preferences are included in the processing and they are accurately interpreted and processed by the applications, and that each step is tamper free. For example, we know how many batches of voting documents per 'combination' are created, so at each step of the processing chain, a match can be made to determine that all known batches are dealt with. The measurable processing steps include roll scrutiny, extracting, vote recording (by hand-wanding, data entry, full page scanning), vote capture for the first time, second vote capture (for checking) followed by reconciliation. Only then will the electoral officer have confidence that the results include all known batches of votes. This would identify, at each stage of the processing, any batches of votes 'missing' or unaccounted for.

Apart from software applications, the infrastructure and the people resources in an overall system are also capable of failure. Where possible, an audit must consider these other non-software resources and the likelihood and impact of their failure on the vote processing.

[1] Control Objectives for Information and related Technology (CobiT©), IT Governance Institute, www.itgi.org

In summary, in an election system, a very important part of this *'end-to-end'* assurance is that voting documents, either individually or in batches, are seen to be processed through all the required steps by all of the component applications and manual processes in the correct sequence.

Checking systems

The *Local Electoral Act* and the *Local Electoral Regulations* require the use of checking systems to provide assurance that each step in the processing and counting of votes and preferences:

- includes all the validly cast votes and preferences; and
- is undertaken accurately.

The *Local Electoral Regulations* provide in *clause 79(b)* for FPP elections…

> *79B Performance standard for checking systems*
>
> *(1) The checking system must ensure that the results of the determination specified in regulation 79(3) are as least as accurate as those that would be produced by…*
>
> *(a) carrying out the following operations manually -*
>
> *(i) rejecting blank voting documents and informal voting documents:*
>
> *(ii) counting votes from valid voting documents; and*
>
> *(b) repeating the operations in paragraph (a); and*
>
> *(c) resolving any discrepancies.*
>
> *(2) In determining whether or not the performance standard in subclause (1) is met, it is sufficient to make reasonable inferences about the errors that are likely to be generated by the operations specified in subclause (1)(a).*

Further, the *Local Electoral Regulations* provide in *clause 104(a)* for STV elections:

> *104A Performance standard for checking systems*
>
> *(1) The checking system must ensure that the preferences recorded under regulation 101 or regulation 102 are as least as accurate as those that would be recorded by…*
>
> *(a) carrying out the following operations manually -*
>
> *(i) rejecting blank voting documents and informal voting documents:*
>
> *(ii) recording votes from valid voting documents; and*
>
> *(b) repeating the operations in paragraph (a); and*
>
> *(c) resolving any discrepancies.*
>
> *(2) In determining whether or not the performance standard in subclause (1) is met, it is sufficient to make reasonable inferences about the errors that are likely to be generated by the operations specified in subclause (1)(a).*

The legislation does not prescribe how the checking is to occur, leaving it to the electoral officer to ensure that appropriate and adequate checking mechanisms exist and are used.

Common points of failure include:

- a human interpreting data from a voting document and entering it into a computer; and
- software automatically processing scanned images of voting documents into votes and preferences.

For these points of potential failure, an electoral officer or service provider must ensure that:

- all human interpretation and data entry is checked at least once by another person. This is normally done by repeated data entry and automated comparison of the two data streams followed by manual data repair where a difference is detected;
- reporting is available that shows the number of differences detected, and the number of corrections; and
- there is a manual process to check that the automated interpretation of votes and preferences includes all validly cast votes and preferences, and produces the correct data.

The auditing of an election system must determine that reasonable processes are defined to:

- provide assurance that all validly cast votes and preferences are correctly presented to and processed by the counting software or STV calculator, and that
- an audit trail exists to demonstrate to third parties, or other interested parties, that the data has been correctly processed.

It is the view of the EWP that good practice requires the use of checking systems at any point in an election system that account for all of the voting documents, their votes and preferences. A checking system based on sampling is not sufficient.

Examples of checking systems

Here are three examples of checking procedures that are typical in running an election:

- two operators independently wand or key votes or preferences from a voting document. The entered data is compared by software and where there is a difference detected, a third person reconciles the difference;
- a voting document is scanned (with a page scanner) and votes or preferences are recognised by software. A person then checks the voting document against the data stored in the computer database. Differences are resolved and the edits checked by another person;
- a computer application produces a report listing all the batches of voting documents that have undergone the initial scrutiny but have not been included in the final results. The batches are located and processed to completion.

It must be stressed that when votes are processed manually, all votes must be processed twice by different persons. This was previously known as the preliminary and official counts. Now the second processing is referred to as the checking system. The results of the two processing streams must be reconciled to ensure accuracy and completeness of the results. For hand-wanding and keyboard data entry, the data must be input twice in separate streams, and then reconciled. For full-page scanning, only one image need be taken, but the image must be processed twice and the votes reconciled. EWP believes that this fulfils the legal checking requirement.

System segmentation

In very simple terms, what the CobiT control model says is that systems can be segmented into processing steps that can be separately verified in operation by comparing the actual outputs to the expected outputs. If each step is shown to be operating correctly, then we can be assured that the whole system is correct from start to finish.

From an auditing perspective, it is also important that outputs from the final step can be reconciled with inputs from a suitable point at the start of the overall process to ensure that no data (voting documents or batches of voting documents) has been lost along the way, between processing steps.

This part of the document illustrates the segmentation of an *'end-to-end'* process for local authority elections. Although they contain some common steps, FPP and STV issue processing is presented separately for clarity.

It is most important to understand that the steps or stages defined in the diagrams below are not necessarily the way that any particular election software suite might break down into its component applications and manual processes. However, given that the legislation identifies some broad steps of in the conduct of an election, we might expect that the breakdown presented below is broadly accurate for the conduct of any election.

In practice, a particular voting document will normally contain some FPP issues and at least one STV issue (for the district health board). Therefore a batch of similar voting documents will provide data that feeds into both FPP vote totalling and STV preference allocation steps. How this is done will depend on the architecture of the processing systems.

Vote processing for an FPP issue

Processing an FPP issue consists of a sequence of the following broad steps:

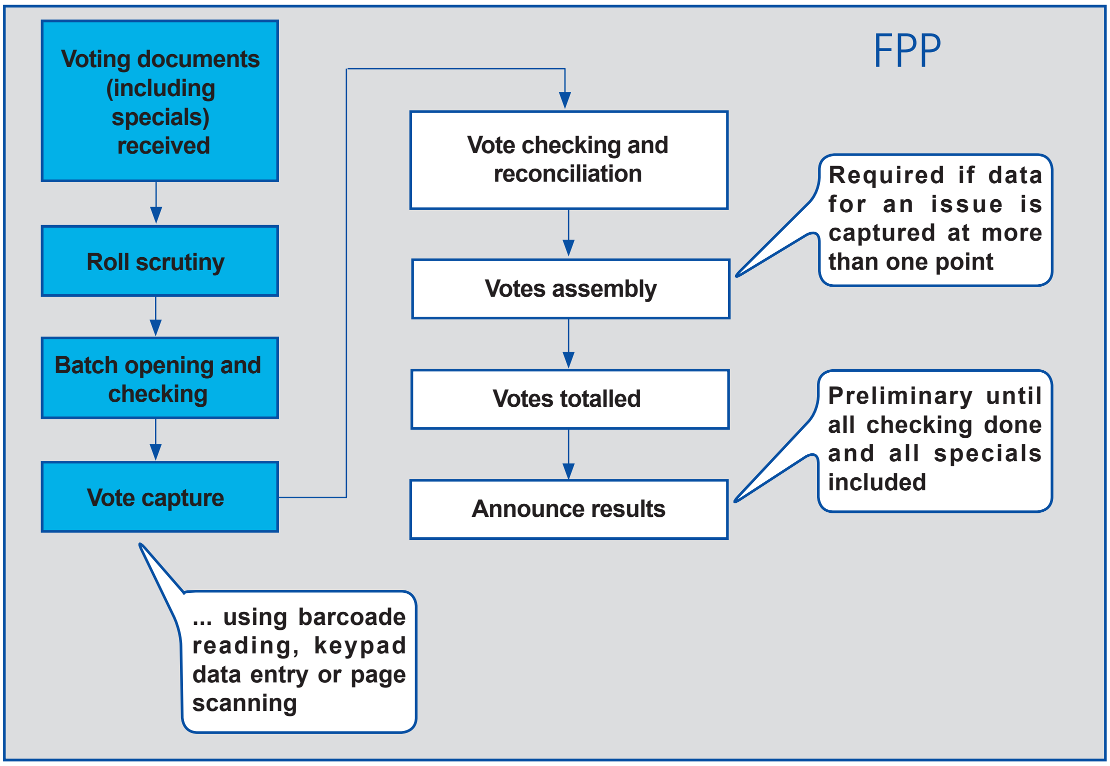

FPP
Voting documents (including specials) received
Roll scrutiny
Batch opening and checking
Vote capture
... using barcoade reading, keypad data entry or page scanning
Vote checking and reconciliation
Votes assembly
Required if data for an issue is captured at more than one point
Votes totalled
Announce results
Preliminary until all checking done and all specials included

Figure 1: A typical FPP issue processing sequence of steps

1. **Roll scrutiny:** Returned voting documents are sorted and batched according to 'combinations' of issues. The elector numbers are entered into the database and recorded as being a member of the particular batch. This means all like voting documents are processed together. Sorting prior to processing is considered essential, so that all like issues can then be identified and easily

managed for example in a judicial recount or inquiry. This step has the following input and outputs…

Inputs: Individual returned voting documents in the unopened envelopes.

Outputs: Batches of unopened envelopes sorted into specific combinations, each batch with a unique batch ID number and a list of electors who have voted.

2. **Batch opening and checking:** Envelopes in a batch are opened then the voting documents are checked and made ready for vote capture. Anomalies such as finding more than one voting document in one envelope are dealt with. Voting documents with problems that will affect vote capture are identified and dealt with. This step is entirely manual. No computer-related processes are required. Note that this is the beginning of the control process in terms of recording the number of documents in each batch and recording anomalies/problems so they can be resolved and processed.

   Inputs: Batches of unopened envelopes with header sheets, sorted into specific combinations.

   Outputs: Secured bundles of voting documents with header sheets, ready for data capture. Control totals (the number of voting documents in the batch) and any other control information will be included on the batch header sheet.

3. **Vote capture:** Each batch is put through a data capture process. The votes marked on the voting documents are recorded in a database. If the data capture is a significantly manual process such as wanding barcodes, the data capture is repeated and both streams of data are presented to the data checking process (see below) for comparison. Note that there must be a checking process in place to ensure that all votes are captured correctly and an audit trail is available.

   Inputs: Secured bundles of voting documents with header sheets, ready for data capture.

   Outputs: Batch details and data in a database.

4. **Vote checking & reconciling the differences:** The captured data is checked, and where there is any difference between the two data streams, the original voting document is checked. Correct data is entered into the database. Inconsistencies and their resolution are recorded in an audit trail.

   Inputs: Data from voting documents that a software test has determined could contain an error.

   Outputs: Correct, verified data with an audit trail.

5. **Votes assembly:** When data is for (some) regional councils and licensing trusts and is being provided from a number of sources, the data streams must be amalgamated before results are totalled.

   Input: Vote data received from various data capture systems.

   Outputs: All vote data ready for totalling.

6. **Votes totalled:** The computer system adds up the votes and reports the results.

   Inputs: Votes in the database.

   Outputs: Election result reports.

Preference processing for an STV issue

Processing an STV issue consists of a sequence of the following broad steps for STV issues. Note that some steps in an overall election system may be contracted out, but the responsibility for the overall system still remains with the electoral officer.

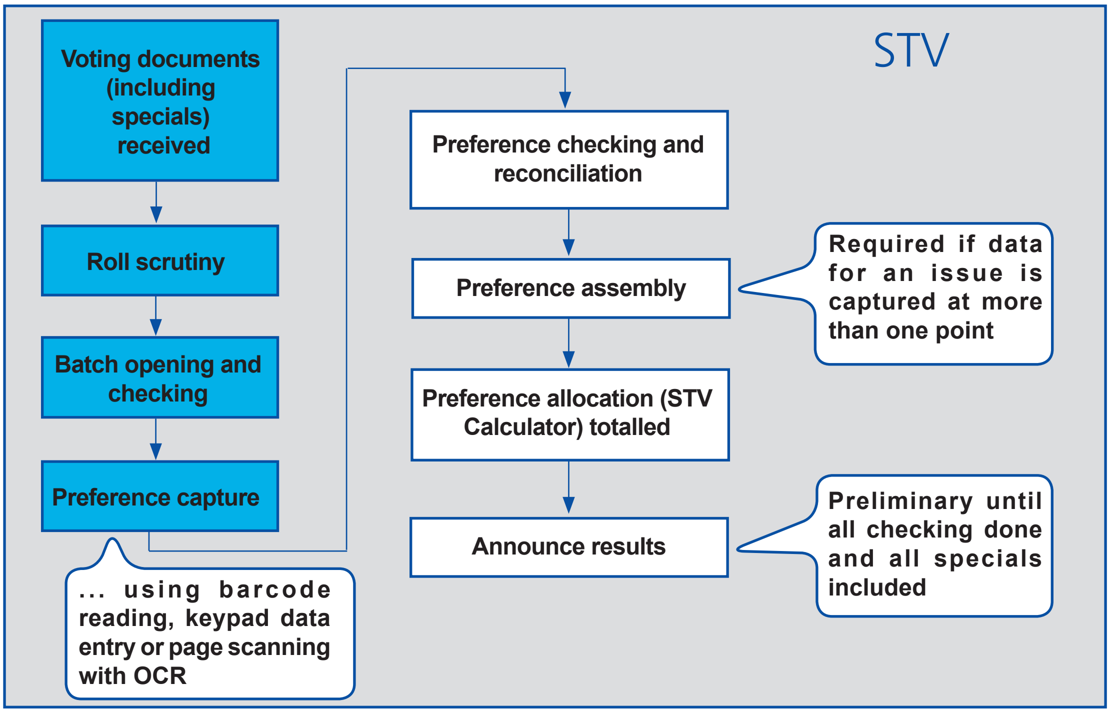

STV
Voting documents (including specials) received
Roll scrutiny
Batch opening and checking
Preference capture
... using barcode reading, keypad data entry or page scanning with OCR
Preference checking and reconciliation
Preference assembly
Required if data for an issue is captured at more than one point
Preference allocation (STV Calculator) totalled
Announce results
Preliminary until all checking done and all specials included

Figure 2: A typical STV issue processing sequence of steps

1. **Roll scrutiny:** Returned voting documents are sorted and batched according to 'combinations' of issues. The elector numbers are entered into the database and recorded as being a member of the particular batch. Sorting prior to processing is considered essential, so that all like issues can then be identified and easily managed for example in a judicial recount or inquiry. This step has the following input and outputs:

   Inputs: Individual returned voting documents in the unopened envelopes.

   Outputs: Batches of unopened envelopes sorted into specific combinations, each batch with a unique batch ID number and a list of electors who have voted.

2. **Batch opening and checking:** Envelopes in a batch are opened then the voting documents are checked and made ready for vote capture. Anomalies such as finding more than one voting document in one envelope are dealt with. Voting documents with problems that will affect vote capture are identified and dealt with. This step is entirely manual. No computer-related processes are required. Note that this is the beginning of the control process in terms of recording the number of documents in each batch and recording anomalies/problems so they can be resolved and processed.

   Inputs: Batches of unopened envelopes sorted into specific combinations with header sheets.

   Outputs: Secured bundles of voting documents with header sheets, ready for data capture.

Control totals (the number of voting documents in the batch) and any other control information will be included on the batch header sheet.

3. **Preference Capture:** The following steps describe wanding or keyboard entry process.

3(a) <u>Preference capture by wanding or keyboard entry:</u> Each batch is put through a data capture process which could be either by hand-wanding or keyboard entry. The preferences marked on the voting documents are recorded in a database. If the data capture is a significantly manual process such as wanding barcodes or keyboard entry, the data capture is repeated and both streams of data are presented to the data checking process for comparison.

Inputs: Secured bundles of voting documents with header sheets, ready for data capture.

Outputs: Batch details and data in a database.

3(b) <u>Preference checking & reconciling the difference of wanded or keyboard-entered preference data:</u> The captured data is checked, and where there is any uncertainty, visually compared with the voting document. Correct data is entered into the database.

Inputs: Data from voting documents that a software test has determined could contain an error.

Outputs: Corrected numerical preference data.

Alternatively, Data capture may be by page scanning.

4. **Preference capture:** The following steps describe the page scanning process.

4(a) <u>Preference capture by page scanning:</u> Each voting document in a batch is scanned and an image generated. The image is held as a file or placed in a database.

Inputs: Secured bundles of voting documents with header sheets, ready for data capture.

Outputs: Images of scanned pages that will be subject to a character recognition process.

4(b) Intelligent character recognition (ICR): The preferences in the voting document images are interpreted by software. Possible errors or uncertainty are flagged for manual checking.

Inputs: Page images.

Outputs: Numerical preference data, some of which is flagged for checking.

4(c) Preference checking & reconciling the differences in ICR data: The captured data is checked, and where there is any uncertainty, visually compared with the voting document. Correct data is entered into the database. Inconsistencies and their resolution are recorded in an audit trail.

Inputs: Page images that are flagged for checking.

Outputs: Corrected numerical preference data with an audit trail.

5. **Preference assembly:** When data is for a district health board and is being provided from a number of sources, the data streams must be amalgamated before results are calculated.

   Inputs: Preference data received from various data capture systems.

   Outputs: Amalgamated preference data ready for presentation to the STV Calculator.

6. **Preference allocation:** The computer system invokes the STV Calculator (developed, certified and licensed by the Department of Internal Affairs) to calculate the results.

   Inputs: Amalgamated preference data.

   Outputs: Results in XML format.

   STV results report. The STV Calculator output is turned into a readable report.

   Inputs: An XML-encoded results text file.

   Outputs: A results report in plain English.

APPENDIX D: ATTACHMENT 2

WHAT TO LOOK FOR IN '*FIT FOR PURPOSE*' SOFTWARE TESTING

An electoral officer and an auditor will need to formally agree on the scope of '*fit for purpose*' IT system testing. The outcome would be a report on the adequacy of the processes and system documentation, functions, features, and test results. It would be expected that an IT system implements the following features and these must be adequately described by the accompanying documentation (the list is not exhaustive but for guidance only):

- clearly defines how the *'end-to-end'* system is segmented into distinct applications and processes and what the purpose of each application and process is. This must include any steps that are entirely manual;

- adequate checking systems exist for every step and application used in the processing of voting documents;

- control points exist and reports are available from those control points and how the reports are intended to be used;

- the whole process allows any particular batch of data and its contained votes or preferences to be easily tracked, and its current state to be identified quickly;

- reports exist that describe how the status of each batch of voting documents and, where necessary, the location and status of any individual voting document can be determined;

- security features exist for confidentiality of voters, the votes and results, in accordance with the existing legislation, regulations and good practice;

- audit trails exist (normally files that list the details of an application's data processing) along with guidance on how they are activated and contents are to be interpreted, and mechanisms to protect against modification or tampering;

- defines the software environment in which the election software is warranted to operate correctly, including service packs and security patches and other software components like anti-virus or security agents;

- defines a suitable hardware environment (eg, workstation and server sizes and speed) necessary to provide satisfactory throughput for elections of various sizes and to provide for redundancy, availability and integrity;

- describes how the software must be installed and configured within the specific required operating environment;

- provides adequate instructions and test data to permit the electoral officer to perform acceptance tests leading to assurance that the system has been configured and is operating correctly;

- describes how to set the security of the system;
- describes how to install and configure any third-party software components (including the operating systems and database software if this is relevant) that are required for the election software to operate, or alternatively, reference satisfactory documentation supplied with the third-party software;
- describes how the election software is to be configured with election-specific parameters (issues, candidates, electors etc);
- defines data volume limits within which the software is warranted to operate correctly. This is particularly important if a service provider intends to simultaneously process an election for more than one local authority on the same platform;
- describes how each module is to be operated in respect of accepting input data, and producing output data output;
- any software module that produces data to be transmitted to another location, does so in a way that labels the data unambiguously, and also produces an audit report and statistics in a form that can be transmitted with the data;
- describes the administration steps that must be taken to ensure the correct operation of each module and to demonstrate that the output and input data is in balance and accounted for;
- adequately describes the meaning of every possible error message and what to do in the event of error occurring;
- adequately describes the steps that must be taken to safeguard the integrity of the data during an election;
- describes the way changes to the processes, systems or data are managed;
- describes the escalation procedures in the event of system or process failures that may impact the election results, timeframe or reputation of the electoral officer;
- adequately describes the steps that must be taken to safeguard the integrity of the data during an election;
- describes the way changes to the processes, systems or data are managed;
- describes the escalation procedures in the event of system or process failures that may impact the election results, timeframe or reputation of the electoral officer;
- documents any other aspects that are vital to a successful election outcome.

APPENDIX D: ATTACHMENT 3

STANDARD OF AUDIT

The New Zealand Institute of Chartered Accountants (NZICA), through its Professional Practices Board, provides a comprehensive set of standards for audit and assurance. Further, the Institute has recently completed its public consultation on the proposal to adopt the International Standards of the International Auditing and Assurance Standards Board (IAASB), including International Standards on Auditing (ISAs), in New Zealand. This body of standards (especially the Agreed-Upon Procedures) represents the best practice in auditing and assurance that is available to guide an audit of an election system in New Zealand. The IAASB standards are being progressively ratified by the NZICA. The process is scheduled for completion in mid-2009.

The SOSLGM Electoral Working Party proposes that every audit of an election system for New Zealand is undertaken in full compliance with the current standards adopted by the Institute to ensure that the audit can be relied upon by the Office of the Controller and Auditor-General.

The diagram below is part of the diagram of the Professional Standards Framework of the Institute of Chartered Accountants of New Zealand.

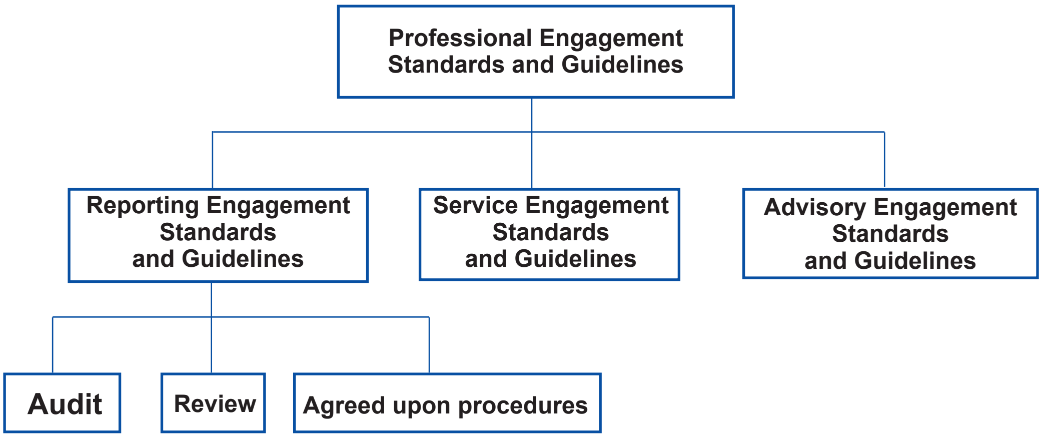

Professional Engagement Standards and Guidelines
Reporting Engagement Standards and Guidelines
Service Engagement Standards and Guidelines
Advisory Engagement Standards and Guidelines
Audit
Review
Agreed upon procedures

Figure 3: New Zealand Institute of Chartered Accountants professional engagement standards and guidelines