Appendix 2H

Risk Analysis

THE POLICY INSTITUTE, TRINITY COLLEGE DUBLIN

Dr. Frank Bannister, *Department of Statistics, TCD*

Table of Contents

1 Summary of conclusions

Risk analysis is concerned not only with the probability of a problem occurring, but also with the impact if it does occur. There are four principal steps involved in preparing a risk analysis:

- Identification of each possible undesirable event;
- Estimation of the probability of it occurring;
- Assessment of the impact if it occurs; and
- Identification of possible actions to prevent, reduce or eliminate the probability of occurrence or take remedial action if it does.

In this instance, as often, in arriving at a judgment, it is appropriate to compare the resultant risks with the risks inherent in the current system or in maintaining the status quo. As no system is ever perfect, **the question is what risks are tolerable or acceptable** in the light of the known problems in the current system.

Viewed through the lens of risk analysis, many of the potential problems raised by some commentators as theoretical possibilities, are in practice not material risks. For example, in examining a theoretical risk of tampering, it is not only necessary to ask *could* it be done, but what is the relationship between the effort required and the benefit to the person tampering with the system? Similarly, a small problem (such as loss of an occasional vote) might be acceptable given considerable improvements in overall accuracy compared with a manual system. It should be noted that in general, the greatest risks in any system come from humans (as opposed to mechanical risks or risks from nature). Furthermore, research shows that it is insiders who generally pose the greatest threats to system security.

The purpose of this analysis is to identify those risks with which the Commission needs to be concerned. In this section, 49 possible risks are analysed. Of these, five are material risks. These are:

- An error in the system as a whole in the June 2004 election (Risks 5.1/5.14/5.15);
- Errors in the voting machine software which affect all machines (Risks 5.3/5.5/5.13);
- Tampering with the software to alter the result of an election (Risks 6.1/6.6);
- Tampering with vote modules during transportation or storage between polling stations, service centres and count centres (Risk 6.4); and
- Damage to machines in between elections (Risks 6.5).

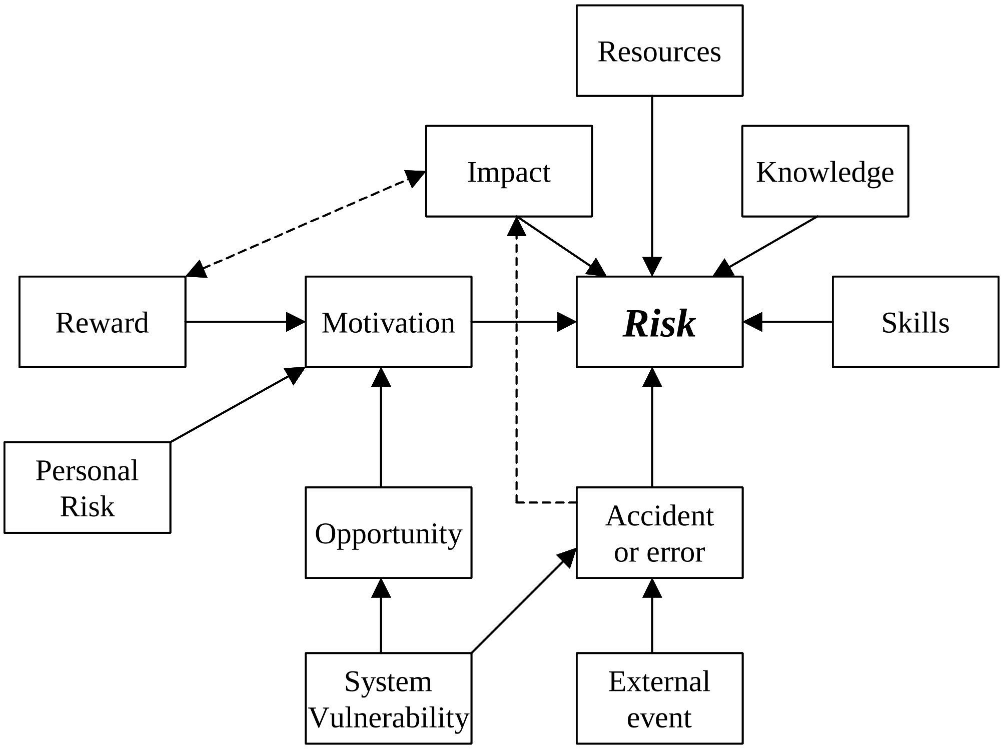
The latter three risks can be considerably reduced, if not eliminated, by appropriate procedures. The first two risks cannot be dealt with this side of the June 2004 election.

Finally, it should be noted that many of the risks identified below only exist because of the absence of an independent verification mechanism for the results such as an audit trail.

2 Analysis framework

The approach used to model the risks in electronic voting is based on two models. The first model (Figure 2.1) shows the factors that create risk.

Figure 2.1 Model of risks in e-voting



The following is a short description of this model with key terms defined as follows:

- ***Reward*** refers to the return or potential gain accruing to somebody tampering with the system.
- ***Personal risk*** is the possible penalty if caught tampering or if the tampering fails.
- ***Impact*** is the extent of the alteration that occurs as a result of malpractice (or of an accident or error).

Both reward and personal risk create a level of motivation, which is the strength of the drive to tamper with the system. This will be moderated by opportunity, i.e. how easy it is to gain access to the system for the necessary time and at the appropriate level. This in turn is determined by system vulnerability, including procedural vulnerability. Malpractice risk is also moderated by the skills of the malefactors, the resources that they have available and the knowledge of the system that they have or can attain.

Finally, external events and system vulnerability also give rise to risks from accident or error.

This second model is a categorisation of risk type on a 2 x 2 grid (Figure 2.2).

Figure 2.2 Categorisation of risks

Systemic	Considerable concern SE	Greatest concern SM
Non systemic	NE Least concern	NM Moderate concern
	Error	Malpractice

2.1 Definitions

The following definitions are used:

Error refers to a fault or problem that occurs by either:

- Hardware failure;
- Software failure or bug;
- Human error; and
- Accident or ‘Act of God’.

Malpractice refers to a problem caused by a deliberate attempt to:

- Alter the result of an election;
- Break the secrecy of the ballot box; and
- Disrupt the election.

Systemic here means that;

- In the case of error:
    - A failure in design or manufacturing that occurs in several or all machines; and/or
    - A weakness in the process, which causes errors at multiple or all locations.
- In the case of malpractice, an attempt to do any, or any combination of, the following:
    - Cause a significant alteration in the votes in one constituency;
    - Alter votes at several or all locations;
    - Find out how many voters voted;
    - Sabotage several machines at one location or many locations;
    - Interfere with the counting software at one or more centres; and
    - Interfere with the transmission of ballots between processes or locations.

Non-systemic means:

- In the case of error, a one off failure, accident or mistake such as the failure of a single machine at a polling station;

- In the case of malpractice, a one-off, local attempt to do any of the things listed above under systemic malpractice, but at a single location.

Table 2.1 summarises the risks examined in this section.

Table 2.1. Summary of risks

Risk	***Description***	***Type***
3.1	Complete machine failure.	NE
3.2	Power failure.	NE
3.3	Single ballot lost.	NE
3.4	Accidental damage to a voting machine	NE
3.5	Single ballot not recorded	NE
3.6	No votes written to module	NE
3.7	Single ballot recorded incorrectly	NE
3.8	Damage to module during transport	NE
3.9	Accidental electromagnetic interference	NE
3.10	Error in data upload in service centre	NE
3.11	Accidental miscounting of votes	NE
3.12	Accidental non abstaining voter identification	NE
3.13	Postal voter identified.	NE
3.14	Disabled voter identified	NE
3.15	Software error in some machines	NE
3.16	“Spoiled” vote (blank ballot) voter identification	NE
3.17	Module accidentally overwritten at service centre	NE
4.1	Single or small number of ballots altered electronically	NM
4.2	Small scale impersonation	NM
4.3	Deliberate voter identification	NM
4.4	Interference with a single or a small number of modules during storage or transportation	NM
4.5	Destruction of or damage to a single or a small number of modules during transportation	NM
4.6	Deliberate damage to a voting machine	NM
4.7	Voter coercion or bribery	NM
4.8	Switching of vote modules	NM
4.9	Switching of votes CD	NM
4.10	Adding votes before opening of polling station	NM
5.1	General system failure	SE
5.2	Widespread loss of ballots	SE
5.3	Widespread ballots recorded incorrectly	SE
5.4	Widespread accidental electromagnetic interference	SE
5.5	Widespread error in data upload in service centre	SE
5.6	Widespread miscounting of votes	SE

Risk	***Description***	***Type***
5.7	Extensive voter vote identification	SE
5.8	Many postal voters identified.	SE
5.9	Many disabled voters identified	SE
5.10	System cannot cope with features of an election	SE
5.11	System cannot cope with number of voters	SE
5.12	Votes accidentally lost during counting	SE
5.13	Inherent fault in voting machine hardware	SE
5.14	Inherent fault in voting machine software	SE
5.15	Inherent fault in counting pc software	SE
5.16	Inherent fault in counting hardware	SE
6.1	Tampering with voting machine software or hardware	SM
6.2	Wide scale impersonation	SM
6.3	Deliberate wide scale voter identification	SM
6.4	Widespread interference with modules during transportation	SM
6.5	Widespread damage to voting machines	SM
6.6	Tampering with count software	SM

2.2 Scales

The following are the scales used to measure various factors.

Probabilities are expressed on a seven point verbal scale only as it is not possible to quantify these. The scale runs:

- Zero (non existent);
- Very low;
- Low;
- Moderate;
- High;
- Very high;
- Certain.

Apart from the fact that assigning numerical values to terms like ‘low’ and ‘moderate’ would only give a spurious accuracy, it is worth noting that the interpretation of language in probability is highly subjective. For example, in betting on an outsider in a horse race, a gambler might consider a probability of 0.8 of losing his or her stake to be a ‘high’ probability, whilst a probability of 0.1 of losing the stage would be ‘very low’ in the circumstances. On the other hand, a probability of 0.1 of an election giving the wrong result would be regarded most people as being completely unacceptable; indeed, even a 0.001 (one in a thousand chance) would be unacceptable to many, if not most, citizens. The assessment of probabilities in this section tries to arrive at as detached and balanced a view of the probabilities as is possible.

Impact is expressed on a four point verbal scale as follows:

None	This will have no impact at all.
Small	This may affect a small number of individual voters, but would not endanger or invalidate the election.
Large	This could result in a wrong result or the election being declared invalid in a constituency.
Catastrophic	This would either invalidate the election, and/or result in severe loss of public trust in the system.

Comparison is based on a five-point scale as follows:

Additional	This is a new risk which does not exist in the current system.
Increased	This risk exists in the current system, but is higher in the electronic system.
Neutral	This risk exists in a similar form in the current system or the net effect on overall risk is broadly neutral.
Decreased	This risk exists in the current system, but is lower in the electronic system.
Eliminated	This risk exists in the current system, but is removed by the electronic system.

Each risk/problem is analysed under the following headings:

- Event;
- Description of the event and the circumstances in which it could occur;
- Probability of the event occurring;
- Impact if the event does occur;
- Comparison with corresponding risk (if any) in the existing paper system;
- Pre-emptive actions which can be taken to reduce the risk; and
- Corrective actions, which can be taken if problem occurs.

This section concludes with a brief discussion of risks in the current system, which would be eliminated by an electronic system and some other risk related issues.

2.3 Important caveats

This analysis works within the parameters of the situation. Specifically, it should be noted that:

- In considering the pre-emptive and corrective actions that can be taken, it is assumed that the State is limited to the facilities provided by the current system and current resources.

- In practice, many, though by no means all, of the risks discussed below would be eliminated if there were a voter verified paper audit trail. However, it should be noted that because of sampling error, small errors in an electronic voting system would be undetectable.

- There are problems in the current system, which do not arise in the new system. Some of the more important of these are discussed at the end of this section. [For further detail, see the report in Appendix L.]

- This section is not concerned with verification of the results after the election except where this relates to recovery from a problem. For this reason, the issue of post election checking is only addressed obliquely. For example, it is possible to check machines before and after an election to increase confidence in the system, but this is not considered a risk analysis issue although it is a potential part of a risk management strategy. The latter is only suggested where it would reduce the relevant risk on the day.

3 Non-systemic errors (NE risks)

Non-systemic errors are the most likely type of problem to occur, in part because there are more possibilities for localised error than anything else. For example, it is virtually certain that one or more voting machines will fail on the day. However, the impact of any conceivable non-systemic error is likely to be immaterial in terms of the overall election and, at worst, is no worse than the equivalent risks in a paper system.

In general, the gains from the elimination of problems (such as accidentally spoiled votes) in the current system outweigh the collective impact of all of these risks.

Risk (3.1) **Complete machine failure**

Description A machine simply stops working, or starts to misbehave in some manner and has to be shut down.

Probability Low for a given machine.
Close to certain for one or more machines in a general election.

In the 2003 Dutch election, 5 machines out of 7,500 gave problems (which were all fixed) on Election Day. If there are 6,000 machines in use during an election and the probability of a machine failing is .001, then it is virtually certain that one machine will fail and the expected number of failures during the day is 6. The suppliers have suggested a conservative reliability factor of .995 implying that the expected number of failures is 30.

Impact Small.

The worst-case scenario would be loss of all votes already entered into the machine. Given the nature of the vote storage the probability of this is virtually zero (see Risk 3.6). More likely is the loss of a single vote at the point of failure (see Risk 3.3). This would not be sufficient to invalidate the election. In a small polling station with only one or two machines, this could cause delays in voting or a hiatus in voting until a replacement machine was available.

Comparison Additional.

Pre-emptive The main risks here can be, if not be entirely eliminated, then at least substantially reduced by having spare machines available. It is important that a replacement machine can be *in situ* within a reasonable timeframe. An alternative would be to extend the time available for voting.

Corrective Replacement of the faulty machine.

Risk (3.2) Power failure

Description Power fails at a polling station.

Probability Low

Impact Small.

The worst-case scenario would be that batteries ran out before the close of polling. This would necessitate extension of polling hours.

Comparison Additional.

Pre-emptive Making sure that sufficient batteries to operate the system are available and are fully charged. Standby generators could be used if necessary, but this is probably excessive.

Corrective Extension of polling time. Bring in fresh batteries.

Risk (3.3) Single ballot lost

Description A vote is not captured by the machine due to machine or power failure at the time, or just before, it is cast.

Probability Low for a given machine.
Close to certain for one or more machines in a general election.

Impact Small.

There is no significant risk to the validity of the election from this.

Comparison Reduced.

There is a small risk of this in the current system at the count centre, particularly if one considers inadvertently spoiled ballots. This is an additional risk, but there is no equivalent risk at the service centre so this is probably positive in its overall impact. Given this, the risk here is probably less than in the current system.

Pre-emption There is no way that this can be avoided.

Correction It may be possible to put a procedure in place to enable a voter to vote again if it can be established that a vote was definitely lost. However, this cannot be guaranteed to work in every case.

Risk (3.4) Accidental damage to a voting machine

Description A machine is damaged (dropped, flooded, hit with a heavy object, etc.)

Probability Low.

Impact Potentially large.

The worst-case scenario would be loss of all votes already entered into the machine. While a loss of data in these circumstances is extremely unlikely, the impact could be significant. It is estimated that the maximum number of votes in a machine could be in excess of 200 by close of poll. This number of lost votes is more than sufficient to change the outcome of an election in a marginal constituency.

Comparison Neutral.

This is also a slight risk in the current system where a ballot box could be set on fire or flooded.

Pre-emption Proper training of staff.
Suitable tables at polling stations.
Good operating procedures.

Correction There is no corrective action that could recover votes lost in this way. The damaged machine can be replaced for the remainder of the day.

Risk (3.5) Single ballot not recorded

Description A ballot is cast, but not written to the voting module.

Probability Very low.

This could happen because of software or hardware error (for example if there was a problem with a bit switch due to electromagnetic or radioactive interference - see Risk 3.9).

Impact Moderate.

The impact here is not the loss of the single vote, but the question mark that it would raise over all ballots cast in the machine in question.

Comparison Increased.

This is a remote risk in the current system, but the impact is negligible.

Pre-emption Thorough testing of the voting machine.

Correction There is no corrective action that can be taken as, while it might be known that a vote was lost, which vote might not be clear.

Risk (3.6) No votes written to module

Description No votes are recorded on the module due to a fault in the voting machine. It should be noted that if this were to happen, there would also be no votes recorded in the back-up module.

Probability Very low to zero.

This could happen because of software or hardware error or because of a fault in the module itself. Given the extensive testing and operational history of the proposed machine, this seems highly improbable.

Impact Large.

This could possibly invalidate the entire vote in the constituency in which it happened.

Comparison Additional

Pre-emption Thorough testing of the voting machine.

Correction There is no corrective action that can be taken if this happens apart from re-running the election in the constituency.

Risk (3.7) Single ballot recorded incorrectly

Description The vote recorded differs from the vote cast.

Probability Very low to zero.

Impact None.

There would be no impact in practice because it can never be known whether this has happened and a single vote accidentally altered will not have a material effect on the election.

Comparison Additional.

Pre-emption Thorough testing

Correction No action possible.

Risk (3.8) Damage to module during transport

Description A vote module is damaged during transport.

Probability Low

Impact Moderate

This would result in a loss of a number of votes, possibly a couple of hundred from a busy polling station.

Comparison Neutral.

This risk is akin to the loss of a box of ballot papers. While damage to a module is more likely than to a ballot box, given the availability of back-up modules, this is neutral.

Pre-emption Back-up modules in machine.
Proper staff training.
Good transportation procedures.

Correction Use back-up module.

Risk (3.9) Accidental electromagnetic interference

Description A bit or bits in the machine are altered by electromagnetic radiation (called a single event upset or SEU). There is a number of other possible ways this could happen which range from a machine in a polling booth being placed close to a transformer, to radioactive decay in a silicon chip, or even cosmic rays.

Probability Very low

Impact Small.

An error of this type should be detected by the voting machine itself, which will shut itself down. Existing votes will be protected.

Tests show that votes in the module itself are unaffected by extremely large electromagnetic fields.

Comparison Neutral.

This is an additional risk, but there are risks with paper ballots as well (such as fire and flood). This is not a materially new risk.

Pre-emption Common sense about machine location.

Correction Bring in a replacement machine.

Risk (3.10) Error in data upload in service centre

Description The votes are correctly recorded on a module, but are mis-read and/or mis-written when transferred into the CD prior to loading onto the count PC. This risk and the following risks are the two most important risks from non-systemic accident/error. In fact, this is probably the most material error of this type as it is possible to re-run a count on a separate machine, but if any errors are made in reading the votes in, the same error may be reproduced in all counts.

Probability Very low

This has been tested, but there are so many possible permutations and combinations that any test can only be partial.

Impact Small

As a once-off error, this might not be detected and, for a single module, is unlikely to have a material impact on the election. However, if it were discovered (say by somebody putting the module into another reader), it could have an impact on public trust and confidence in the system and could have significant political implications.

Comparison Additional
There are problems with the current paper system with votes being misread by manual count staff. However, a whole series of votes in one location being systematically miscounted is not likely.

Pre-emption Testing of reader before and after reading.
Test in a separate reader.

Correction Replace reader.

Risk (3.11) Accidental miscounting of votes

Description An error in the count software gives the wrong result.

Probability Very low

Impact Catastrophic. A fault here could invalidate the election and would almost certainly result in a total loss of public trust.

Comparison Reduced
The electronic system is not transparent and cannot be seen by tallymen. It is not possible to be certain that the result is the correct one except by a parallel run. However, there are different and arguably more serious problems with the manual count, though the possibility of wholesale error is small.

Pre-emption Testing of the software.
Making the votes available to others to count.

Correction Votes could be made available to independent third parties after the election. They can then be re-counted using other machines and software. This provides a degree of comfort, but should such a re-count arrive at a different result, there could be serious ramifications even if, eventually, the recount software turned out to be faulty.

Note also that if, due to concerns about secrecy, only partial votes were released, it would be difficult to correct this error with certainty (see Risk 4.7).

Risk (3.12) Accidental non-abstaining voter identification

Description An individual voter’s vote becomes known to others. This could arise from a regulation, which allows a returning officer to release details of the votes in a particular polling station.
There is also a minor concern about the different ‘beeps’ given by the machine telling third parties that voters had made mistakes while voting.

Probability Very low

Impact Moderate

Comparison Neutral

This could (in theory) happen under the current system.

Pre-emption Change the regulations to prevent returning officers releasing votes or only allow them to do so if there are more than a certain number of votes in a polling station, say 500. It is understood that this policy is being considered by the Department of the Environment, Heritage and Local Government.

Clear guidelines for returning officers.

Correction Not applicable.

Risk (3.13) Postal voter identified

Description The vote of a postal voter is identified.

Probability Low

Unlike the current system, postal votes will have to be keyed into a system by a third party. It is possible that a postal voter’s vote, especially from a small community, could be identified under these circumstances, especially as local election agents are entitled to be present to check that votes are correctly entered.

Impact Large

While this would not affect the outcome of the election, this could become politically contentious.

Comparison Increased

There is some small risk of postal voter identification in the current system, but this risk is higher in the proposed system due to the need to re-key.

Pre-emption There is no way that this can be avoided apart from adopting tight procedures and, for example, requiring that agents present to verify that votes are typed correctly are from outside the constituency.

Correction Not applicable.

Risk (3.14) Disabled voter identified

Description A disabled voter's vote is identified.

The voting machine is going to be more awkward for some voters to use (though it may be easier for others).

Probability Low to moderate.

Impact Large.

Disabled voters are entitled to the same secrecy as everybody else.

Comparison Increased

The system is designed to tilt so a wheelchair user can key in his or her vote. Blind voters can have a companion present. It is probable that some disabled voters who could manage paper voting will need assistance to operate the voting machines. There is therefore a small increase in risk here.

Pre-emption There is a facility on the Powervote machine to have audio feedback for visually impaired voters. This could be put into operation.

Correction Not applicable.

Risk (3.15) Software error in some machines

Description Each machine has to be configured for a specific constituency. It is possible that in doing this, a software error could give an incorrect result in a particular constituency because of the combination or number of candidates.

Probability Low

The problem arising in relation to this is testing. There are too many possibilities to test every eventuality so there is some residual risk that a particular combination of candidates or elections could cause a problem.

Impact Large
This could distort or give the wrong result in a constituency.

Comparison Additional

Pre-emption One way to test for this would be to run a dummy election the day before with the machine configured as for the election.

Correction No short term corrective action possible.

Risk (3.16) “Spoiled” vote (blank ballot) voter identification

Description A voter who does not cast a vote can be identified by the returning officer and possibly by third parties as the machine has to be re-set after such a vote.

Probability High

Impact Moderate to large

While a majority of spoiled votes in the current paper are probably errors made by voters in completing ballot papers a certain number of votes are deliberately spoiled or left blank. The system makes no provision for casting a blank ballot, but it is possible to obtain a token, have the machine activated and then simply walk away without pressing the ‘cast vote’ button. When this happens, the system must be re-set by turning a key on the control device. This action is quite visible to the public (and of course, to the official concerned). Consequently, such ‘voters’ would have no certainty of anonymity. This may raise legal issues and a possible constitutional challenge on the right to cast a blank ballot.

Comparison Additional

Pre-emption This problem can be surmounted by modifying the voting machine software. This should not be difficult to do.

Correction Not applicable.

Risk (3.17) Module accidentally overwritten at service centre

Description There are two keys needed for the programming and reading unit (PRU). A red key is used for the reading slot and a black key for the programming slot. The latter slot is used for configuring the module for the upcoming election. Both keys must be turned on to either read or program. This could give rise to an accidental overwriting of a module at the service centre if a module were accidentally put in the programming rather than the reading slot.

Probability Low

Impact Small

Votes in the module would be lost. The impact would depend on the number of votes in the module and how marginal the constituency was.

Comparison Additional

Pre-emption The system should be redesigned so that two keys are needed for programming while only one is needed for reading the modules.

Another possible solution is that, prior to reading in the modules, the programming lock is turned on, and the key removed. While locked, it is not possible to enter a module into the programming slot. In this situation, only the red key is needed from then on, and the black key could be left in a secure location to prevent accidental erasing of data by reprogramming it.

Correction Not applicable.

4 Non-systemic malpractice (NM risks)

With the exception of deliberate sabotage, non-systemic malpractice is the least likely of the four problem classifications to occur. The reason for this is that the effort involved in altering a single machine is disproportionate to any possible desired outcome. Apart from the fact that tampering with a single machine is difficult, it is not possible to know which or how many voters will use that machine on the day. There is, therefore, little motivation for trying to alter votes in this way.

Risk (4.1) Single or small number of ballots altered electronically

Description An individual ballot or a small number of ballots is electronically altered.

Probability Zero

To do this would involve altering the programming of an individual voting machine. This is possible in theory, but would be extremely difficult to do in practice, as it would require a conspiracy of a number of authorised officials, a high level of skill and considerable access. The likelihood of this is close to zero given that it would have little effect in terms of affecting the outcome of an election. If this were done systematically however, the situation would be quite different (see below).

Impact Small

Comparison Reduced

It is probably easier to do this with a paper ballot so the risks are less than the current system.

Pre-emption Good security.

Proper and secure storage of modules and machines.

Correction Not applicable. If done skillfully, it would not be known that ballots had been changed.

Risk (4.2) Small-scale impersonation

Description A voter claims to be somebody else and casts more than one vote. This may include legitimate non-voters or people not ‘entitled’ to vote (such as somebody recently deceased).

Probability Moderate

Impact Small

Comparison Neutral

This risk is the same in the current system.

Pre-emption This is not an issue specific to voting technology. It relates to maintenance of an accurate register of electors and good identification checks in polling stations

Correction Not applicable.

Risk (4.3) Deliberate voter identification

Description A person seeks to find out how a specific voter has voted.

Probability Very low.

Impact Small

Comparison Increased.

There is some increased risk in the electronic system from a sniffer device or from the fact that there is an electrical link to the returning officer’s control panel from whence a voting machine is activated. There is a more material risk in a small polling station that a voter could be identified and linked to a particular vote (see Risk 3.12).

Pre-emption Redesign of the activation station so that there is no display screen. This could be done by using a series of lights to indicate status rather than the current readout.

An alternative is to test the system to ensure that it is not possible to ‘sniff’ a vote and to check that it is not possible to transmit a message from the voting machine to the returning officer’s console.

Changing the rules about vote release in small polling stations (see Risk 3.12).

Correction Not applicable.

Risk (4.4) Interference with a single or a small number of modules during storage or transportation

Description An attempt to alter the votes on a voting module during transportation from the polling station to the service centre.

This is one of the more serious risks, particularly if done systematically (see Risk 6.4). It is conceivable that somebody could develop a device to read the data on a module and then re-write it onto the module in such a way as to alter the ballots whilst leaving the internal checksums correct. This would require a high degree of skill to prepare and a conspiracy of several authorised staff, possibly including a member of the Garda Síochána, to execute. Once done, there would be virtually no way of discovering the alteration.
As noted above, the rationale for doing this to a single module is questionable. Doing this on an extensive scale is a different matter.

Probability Low.

Impact Large.

This could be used to alter the result in a constituency, particularly a marginal one.

Comparison Increased.

This is a risk in the current system (stuffing the ballot box). However, ballot box stuffing is difficult; electronic systems make such an exercise much quicker and therefore easier to do.

Pre-emption The most important step required in relation to this risk is to implement good procedures so that modules are not out of view of authorised officials at any time. Further protection could be attained by encryption of the data in the module.

Correction If uncovered, use of the back-up module.

Risk (4.5) Destruction of or damage to a single or a small number of modules during transportation

Description An attempt to steal, destroy or damage a voting module during transportation from polling station to service or count centre.

This type of action is likely to be more taken by a disgruntled employee than anybody else.

Probability Moderate.

While the probability of any given module being damaged is tiny, the cumulative risk is more material. For example, if there is only a probability of 0.0001 that a given module is damaged, given 6,000 modules there is a 0.45 probability that at least one module will be damaged during an election.

Impact Small.

This is only a problem if the back-up module is faulty.

Comparison Neutral

This is a risk in the current system, but the small size of vote modules makes them vulnerable to theft and/or damage in a way that current ballot boxes are not. The availability of a back-up module counterbalances this risk.

Pre-emption The most important step in relation to this risk is good procedures so that modules are not out of view of authorised officials for any period of time. Back-up modules must also be protected.

Correction Use the back-up module.

Risk (4.6) Deliberate damage to a voting machine

Description An attempt to damage a machine either by physical assault or by magnetic or electromagnetic interference.

Probability Low.

It is possible that political extremists or others who are out to prove a point about the unreliability of the technology could try to damage a machine in a polling station. There is also a risk to machines in storage between elections.

Impact Small
Given the design of the machine, it is unlikely that votes already cast would be lost in such an attack.

Comparison Additional

Voting machines are obviously more vulnerable than ballot boxes although it would be easy to set fire to a ballot box if one was determined to do so.

Pre-emption Good security on site.

Correction Provide a replacement machine.

Risk (4.7) Voter coercion or bribery

Description A voter is bribed or intimidated into voting in a particular way.

What makes this possible is the use of so-called ‘low preference signatures’. As an example of how this works, consider an election with 10 candidates. A voter is told how to vote down the ballot paper. The intimidator or briber is only interested in the first four preferences, but he puts the last six in a specific sequence so that later, when the ballots are published, he can locate that vote and ensure that the first four are ‘correct’.

Probability Low to moderate.

This would normally seem an implausible scenario. However, intimidation at election time is not unknown in Ireland and there has also been one known case of something quite similar to this being done in Italy with an e-voting system.

Impact Moderate

This would have to be done on a considerable scale to be worthwhile. However, in a marginal constituency it could change the result.

Comparison Increased

This is a theoretical possibility with the current system, but impractical in reality.

Pre-emption Do not publish all votes. If it is not possible to verify such votes, there is no point in using this practice. However, doing this would have implications for re-counts by third parties (see Risk 3.11).

Correction Not applicable.

Risk (4.8) Switching of vote module(s)

Description A vote module or modules is switched for a pre-setup module, either at the polling station or at a service centre.

Probability Low.

This could only be done by an insider. It would require considerable skill and timing, but is feasible.

Impact Moderate

This could change the result in a marginal constituency. It would be difficult to do on a scale sufficient to change an overall election result.

Comparison Increased

This is a theoretical possibility with the current system, but impractical in reality.

Pre-emption Tight procedures.
Two authorised officials present at all times with modules.

Correction If discovered, go to back-up module.

Risk (4.9) Switch of votes CD

Description The CD with the votes generated at the service centre is switched with a CD prepared earlier or with another CD written subsequently.

Probability Very low to zero.

This is feasible, but would be virtually impossible to execute plausibly in the time available.

Impact Large.

This would alter the result in a constituency.

Comparison Additional.

Pre-emption Tight security.
Careful checking of all checksums etc.

Correction If discovered, re-create correct CD

Risk (4.10) Put in additional votes at start of poll

Description There is an opportunity for corrupt officials to ‘vote’ a number of times before the polling station opens to the public.

Probability Low.

This is easy to do, given collusion by a number of officials, but it would require a conspiracy of several people. At the close of poll, the ‘extra’ voters could be selected from non-voters on the day who are on the voting register.

Impact Small

This might alter the result in a constituency, but the impact would be marginal in most cases.

Comparison Additional

Pre-emption Careful vetting of officials
Good procedures.

Correction None possible, if done carefully, this would be undetectable.

5 Systemic errors (SE risks)

This type of error is less likely than a local error, but much more serious if it occurs. A systemic error, particularly a problem with the voting machine or the system as a whole, could result in an incorrect election result, an election being abandoned or loss of public trust.

All of these risks are additional; none exist in the present paper system.

Risk (5.1) General system failure

Description A general failure of the system to operate though failure of one or more components. This is the single largest risk in the system, particularly for the scheduled elections in June 2004.

Probability Low (long term) to moderate (short term)

This is a serious concern in the short run because of the limited testing of certain parts of the system and because of the absence of both end-to-end (systems) tests or a parallel run. It is highly unusual for a system of this size and importance to be implemented without either a systems test or a parallel run. The pilot run in three constituencies in the last general election was not a parallel run as it was for a different machine configuration and the results were unverified and unverifiable.

The present system depends on a number of components including Microsoft Windows 2000 and Access 2000, two products, which are not without security problems. Window 2000 has been the subject of many attacks and is subject to constant update and patching to fix holes in the software.

Impact Catastrophic

This would almost certainly either invalidate the election or cause it to be aborted.

Comparison Additional

Pre-emption Full system testing
Parallel run of the system.
Clearly the above cannot be done before June 2004.

Correction None apart from re-running the election.

Risk (5.2) Widespread loss of ballots

Description Ballots are cast, but not written to the voting module.

Probability Very low

This could happen because of software or hardware error (for example, if there was a problem with a bit switch due to electromagnetic or radioactive interference from, for example, a solar storm - see below). It should be noted that, short of using formal methods of system development, it is never possible to be certain that software with the amount of lines of code which this software has, is error free. Given the testing to date and the track record of the voting machine, the probability of failure occurring at this point is quite low.

Impact Catastrophic
Such an event would almost certainly invalidate the election and, depending on circumstance, result in a complete loss of public trust in e-voting.

Comparison Additional

Pre-emption Thorough testing of the voting machine by independent sources with full access to source and machine code.

It should be noted that this includes a full retest with every release of, or modification to, the software.

Correction Re-run the election.

Risk (5.3) Widespread ballots recorded incorrectly

Description The votes recorded differ from the votes cast.

Probability Very low.

Impact Catastrophic

A major issue here is that, unlike the loss of paper ballots, there may be no way of knowing that this has occurred unless the distortion is so significant that the consequent results are implausible. The only guide will be pre-election opinion polls, which are not reliable in this regard.

An additional difficulty arising in relation to this is that, if an unexpected result (such as a major upset) were to occur in a constituency, it might give rise to allegations of error or malpractice. There will be no way of either proving or disproving such allegations.

Comparison Additional.

Pre-emption Thorough testing of the voting machine by independent sources with full access to source and machine code.

There are arguments for and against releasing all code into the public domain. On the positive side, it increases public confidence and is more likely to lead to identification and correction of errors. On the negative side, by making the code widely available there would be a greater level of knowledge available to those who may wish to tamper with the system or (say) plant a virus in the PC in a count centre. It should be noted that this also requires a full retest with every release of, or modification to, the software.

Correction None apart from re-running the election.

Risk (5.4) Widespread accidental electromagnetic interference

Description Extensive disruption of machines caused by electromagnetic interference.

This is technically feasible if there were, for example, a major solar storm on the day of the election. There is no protection again such an occurrence but as such storms are normally foreseeable and are unlikely to upset the machines anyway, this possibility can probably be disregarded.

Note that this is only a risk with the machines. The modules seem to be impervious to powerful magnetic fields.

Probability Zero

Impact Catastrophic.

In such circumstance, the election would have to be declared void.

Comparison Neutral.

This is an additional risk, but there are risks with paper ballots as well (such as fire and flood). This is not a materially new risk.

Pre-emption Keep machines clear of sources of electromagnetic fields.
Good shielding.

Correction Re-run the election.

Risk (5.5) Widespread error in data upload in service centre

Description A software or hardware error means that while the votes are correctly recorded on modules, they are read incorrectly into the PCs prior to counting. The same comments made for non-systemic errors of this type apply in this instance, though the implications are much more serious.

Probability Very low

Impact Catastrophic

Again, this might be difficult to detect unless the distortion was sufficient to raise questions in the minds of party officials.

Comparison Increased
There are undoubtedly some errors in the current system however, unlike the manual system, an electronic system has the potential for a massive error.

Pre-emption Testing of readers before and after reading.

Correction Replace readers.

Risk (5.6) Widespread miscounting of votes

Description An error in the count software gives the wrong result.

Probability Very low

Impact Catastrophic.

A fault here could invalidate the election and would probably result in a complete loss of public trust.

Comparison Reduced

See comments on Risk 3.11.

On balance, in relation to this issue, the impact is to reduce risk. While there is some remote risk of software error, if it functions according to specification, the electronic counting system, unlike the current manual system, will be accurate. The option to use fractional votes is also available to eliminate sampling error.

Pre-emption Testing of the software.
Making the votes available to others to count.

Correction Votes are made available to third parties to re-count after the election. See also comments on failure at one service/count centre.

Risk (5.7) Many (ordinary) voters' votes identified

Description The votes of large numbers of voters become known to others.

Probability Very low
See the discussion of voter identification codes using lower preferences (Risk 6.3).

Impact Small

This could be embarrassing rather than anything else.

Comparison Increased

This is a small risk in the current system.

Pre-emption Change the regulations to prevent returning officers releasing votes (or only allow them to do it if there are more than a certain number of votes in a polling station, say 500).

Correction Not applicable.

Risk (5.8) Many postal voters' votes identified

Description The votes of several postal voters are identified.

Probability Low.

See comments under Risk 3.13.

Impact Large.

If this were to occur, it would cast doubt on the secrecy of the ballot.

Comparison Increased
This is a risk in the current system but this risk is increased by the need to re-key in the presence of election agents.

Pre-emption See risk 3.13.

Correction Not applicable

Risk (5.9) Many disabled voters' votes identified

Description The votes of a large number of disabled voters are identified

Probability Low

See comments under Risk 3.14

Impact Small

Comparison Neutral

Pre-emption See comments under non-systemic errors. See risk 3.14.

Correction Not applicable

Risk (5.10) System cannot cope with features of an election

Description The software or hardware cannot handle the particular features of an election (e.g. too many parties, too many candidates, etc).

Probability Low
It is reasonable to assume that the specification has anticipated all possible scenarios at a macro level; however, it is impossible to envisage every possible sequence of events during an election.

Impact Large to catastrophic

In the wrong circumstances, this could cause an election to be abandoned. See also comments above about general systems failure.

Comparison Additional

Pre-emption Thorough testing.
White box testing.

Correction No actions possible.

Risk (5.11) System cannot cope with number of voters

Description There are two scenarios where this could happen. Due to the slow pace of voting, voters cannot get to a machine or due to the high volume of votes cast, the system cannot deal with the throughput. Note that this is more likely to be a problem in the June 2004 election as people become accustomed to the system. In the longer term, voting may actually be quicker using this method.

Probability Very low

However, if a machine or machine failed at a busy polling building, there could be problems.

Impact Small

Comparison Additional

Pre-emption Have replacement or additional machines available.

Correction Extend polling hours.

Risk (5.12) Votes accidentally lost during counting

Description The vulnerable point here is where votes are read from the modules into the service centre PC and to a lesser extent into the count PC. A loss of votes subsequent to this could arise from a failure in the count software or a hardware failure on the PC

Probability Low

See comments on Risk 3.13.

Impact Small/Large
A failure of this nature is immediately visible. If it is a hardware failure, the impact will be small. While there might be some delay while equipment was replaced, the impact should not be material. A software failure (which is much less likely in this particular case) would be much more serious and could cause a count to be postponed for a long period while the problem was resolved.

Comparison Additional

Pre-emption Testing.
Replacement equipment available.

Correction Replace faulty equipment.

Risk (5.13) Other inherent fault in voting machine hardware

Description An error in the hardware design leads to many machines malfunctioning on the day.

Probability Low to zero.

As before, the extensive testing and history of the machine makes this a very low probability.

Impact Catastrophic.

This could return a completely incorrect result for an election.

Comparison Additional

Pre-emption Thorough testing.

Correction No action possible short of re-running the election.

Risk (5.14) Other inherent fault in voting machine software

Description A bug in the machine software causes it to fail or malfunction (see risk 5.3 for the specific instance of miscounting).

Probability Low to moderate.

From information available on the testing of the system, this must be considered a low to moderate risk. This risk will also recur each time the software is altered, as it will have to be fully retested. Furthermore, as there has been no 'white box' testing of this system, this risk is higher than it would be had there been white box testing.

Impact Catastrophic

This could cause a problem during an election and/or return the wrong result.

Comparison Additional

Pre-emption White box testing.

Correction No actions possible short of re-running the election.

Risk (5.15) Inherent fault in counting PC support software

Description The votes are recorded and transferred correctly, but the PC fails or malfunctions due to problems with the operating, database or other software.

Probability Low to moderate

This is also one of the more significant probabilities. There are several things that could go wrong in relation to this including the count software, the operating system, the Access database and so on. The technical environment for counting software is not the best available (see also comments under Risk 5.1).

Impact Large to catastrophic

The ability of third parties to re-run the count reduces the risks here somewhat. However, was it to be discovered, it might cause major political problems about the status of the 'elected' government.

Comparison Additional

Pre-emption Thorough testing.
Allow independently certified agents to re-do the count on their equipment.
Publish counting software (source and compiled).

Correction Replace count software.

Risk (5.16) Inherent fault in counting hardware

Description A hardware problem causes an error in the count.

Probability Almost Zero

Some commentators have raised this issue however, it is so small a risk as to be negligible.

Impact Catastrophic if undetected.
Small if detected.

Comparison Additional.

Pre-emption None possible
Correction Have replacement machines available.

6 Systemic malpractice (SM risks)

In the longer term, this is the area of greatest concern. It is of concern for two reasons. First the impact of this would be widespread; secondly, sabotage apart, it is hidden and therefore difficult to detect. Some parts of the system are more vulnerable than others. The part of the system based in and around the service and count centres is of particular concern. On the other hand, there are steps that can be taken to significantly reduce each of these risks.

Risk (6.1) Tampering with voting machine software or hardware

Description The hardware or (more likely) the software of the voting machine is altered in such a way as to alter votes either *ab initio* or on instruction (e.g. by pressing a certain combination of keys on the keyboard).

Probability Very low

For this to happen requires motivation, skills, conspiracy and opportunity. There is ample historical evidence of motivation to tamper with elections (witness recent events in the USA). The skills are available and it is not difficult to envisage a conspiracy to alter the software. The primary problem is opportunity. This would require either suborning a programmer working for NEDAP or accessing the machines between elections. Neither of these is impossible although the latter would require a formidable degree of organisation and corruption. The conspirators would also have to have already done this or wait until the next software upgrade of the voting machine software as this software is burnt into the hardware of the machine.
While this is an implausible scenario, it is not impossible.

Impact Catastrophic
The problem here is that, if this is done with sufficient skill, it might never be detected. It is important to bear in mind that such tampering would necessarily be subtle, i.e. it would make minor changes to the votes so as not to be too obvious.

Comparison Increased

In theory this is possible with the current system, but in practice it would be almost impossible to execute on any scale.

Pre-emption Good security and testing of code with each new release of software.

Removal of party identification information from the machines. Although this is not foolproof (by pressing certain key combinations, it would be possible to prime the machine), it would considerably reduce this risk.

Correction If detected, re-run the election. Note that if the tampering was done skilfully, it might never be known that ballots had been changed.

Risk (6.2) Wide scale impersonation

Description As for local impersonation, but done systematically and on a wide scale.

Probability Moderate

Impact Small

Comparison Neutral. This risk is the same in the current system.

Pre-emption As already noted, this is not an issue specific to voting technology.

Correction Not applicable.

Risk (6.3) Deliberate wide scale voter identification

Description An attempt to find out how a large number of people voted.

Probability Zero.

Given the design of the system this would be exceedingly difficult to do. While, at some theoretical level it is possible that the ‘pseudo randomization’ of vote storage on the module could be replicated, the skill needed to do this and the effort of noting who voted at which station and in what order bears no relation to any benefit obtainable. This is not a plausible risk. There is a minor risk from sniffing devices, but this is so low as to be negligible.

Impact Large.

Comparison Neutral.

Pre-emption Careful checking for illegal devices during polling.

Correction Not applicable.

Risk (6.4) Widespread interference with modules during transportation

Description An attempt to alter the votes on several voting modules during transportation from polling station to service or count centre.

As noted above, this is a serious risk, but one which can be neutralised by good procedures. In fact this may well be the most vulnerable point in the system for somebody who wants to tamper with an election result. However, it would require a conspiracy on a large scale as well as considerable technical expertise to carry this out.

Probability Low.

Impact Large.

This could be used to alter the result of an election. If done skilfully, it would be undetectable.

Comparison Increased

As already noted, this is a risk in the current system (stuffing the ballot box). However, the electronic system makes such an exercise much quicker and therefore easier to do.

Pre-emption Good procedures including vetting of personnel and tight security in handling modules. Sealing modules in a box where they are held during transportation or if necessary overnight.

Further protection could be attained by encryption of the data in the module.

Correction If uncovered, use of the back-up modules.

Risk (6.5) Widespread damage to voting machines

Description An attempt to damage several machines either by physical assault or by magnetic or electromagnetic interference.

Probability Very low

This seems unlikely to happen on any large scale although it is possible that some machines might be attacked.

Impact Small

Given the design of the machine, it is unlikely that votes already cast would be lost in such an attack.

Comparison Additional

The voting machines are obviously more vulnerable than ballot boxes to damage. However, widespread damage to machines would require a considerable degree of organisation to undertake.

Pre-emption Good security on site.

Correction Having replacement machines available.

Risk (6.6) Tampering with count software

Description The counting software is altered so as to give an incorrect result.

Probability Low

In the longer term, this is one of the major risks of the present approach. There are three important issues here and it is worthwhile examining each in a little more detail.

First, it would be relatively easy to modify the software to give an untraceable advantage to a particular party. This might be done during the randomising process by (say) running several randomisations and picking the one most favourable to a particular party. It might also be done by altering votes as they are read into the system.

Secondly, the problem is amplified by the proprietary nature of the code. Because neither the public nor the department have access to the source and corresponding compiled code, there is no way of checking that such an alteration has not been made.

Thirdly, there may be a window of vulnerability in the process for loading the count software onto the PC. Unless watertight procedures are put in place to ensure that the tested system is the one used on the day, it may be possible to swap versions. This problem is exacerbated by the high rate of change currently taking place in the software.

Impact Moderate to large

This could alter the outcome of the election in a constituency or even a complete election.

Comparison Additional

Pre-emption Make the software open source.
Permit white and black box testing of all software.
Version control procedures for master copies of software.
Tight controls on PCs.

Correction None as, if done properly, this could not be traced.

7 Other risk related issues

There are some risks in the current paper balloting system, which an electronic system will eliminate. These risks are:

1. Inadvertently spoiled ballots;
2. Errors arising through misclassification of votes by returning officers;
3. Errors arising in counts due to misreading of ballot papers; and
4. Different results on re-counts due to the preceding two factors.

In addition, were the system to be used to compute all votes and allocated fractional votes (the Gregory method), the risk of an incorrect result due to sampling error could be eliminated. Some commentators have argued that a result where the difference between candidates is less than the sampling error should be deemed to be a tie.

There is also a risk that voters may accidentally lose lower preferences due to the way the system works when you cancel a preference by pressing a button a second time. This (logically) clears all subsequent preferences. The voter must re-enter these. As voters sometimes switch preferences between two candidates in the paper system, they need to be aware that if they do this in the electronic system, they need to be careful.

Finally, there is a risk that where there are multiple votes to be cast (as is proposed for the elections taking place in June 2004), voters may inadvertently press the “cast vote” button prematurely thus partially disenfranchising themselves.