# Appendix 2F

# Assessment of Risk and Controls

DUBLIN CITY UNIVERSITY

Dr. Ciarán Ó hÓgartaigh, *DCU Business School*
Mark Kenny, *DCU Business School*
Eileen Townsend, *DCU Business School*
Professor John Chandler, *University of Illinois – Urbana-Champaign*

## Table of Contents

**Glossary:**

| | | |
|---|---|---|
| CoEV | - | Commission on Electronic Voting |
| DoEHLG | - | Department of Environment, Heritage and Local Government |
| ECRO | - | European Constituency Returning Officer |
| ELRO | - | European Local Returning Officer |
| EMS | - | Election Management System |
| IES | - | Integrated Election Software |
| LRO | - | Local Returning Officer |
| PO | - | Presiding Officer |
| PRU | - | Programming/reading unit |
| RO | - | Returning Officer |
| VM | - | Voting Machine |

## Executive Summary

We reviewed the significant control procedures of the election management system ('EMS') with a view to highlighting key risk factors and reporting to the Commission on the extent to which these risk factors can be mitigated by existing or additional control mechanisms. The scope of this element of the work excluded IT processing controls. For the purposes of our review, we based our work on documentation provided by the Commission and the Department of the Environment, Heritage and Local Government (DoEHLG) and discussions with the Assistant Principal (Franchise) at the DoEHLG.

A review of the effectiveness or adequacy of the hardware and software comprising the EMS is outside the scope of this review: even if the control procedures described here are adequate and/or if the recommendations contained herein are implemented, the integrity of the hardware and software involved is fundamental to assuring the secrecy and accuracy of voting under the proposed system. Our report assumes that the software, machinery, PCs and other computer-related resources have been tested and verified as operating as intended and primarily assesses non-IT controls which could potentially prevent error and/or tampering.

An effective means of providing assurance regarding the controls surrounding the system is to assess the potential effectiveness of input and output controls before, during and after voting. The review carried out by us has raised a number of concerns regarding the level of controls in place in that context. These concerns are discussed in further detail in the body of this report. They include, in particular but not exclusively, concerns regarding:

- the storage of the components of the voting machine in advance of programming;
- the efficacy of controls surrounding the sealing of ballot modules in the voting machines; and
- the level of controls surrounding the PCs and CDs used to read and record the votes from ballot modules.

We relied to a great extent on procedures manuals provided to us in the course of our work. In many cases, those manuals set out procedures to be followed when the system worked but were less detailed in describing procedures to be followed in the case of system problems or failure. This may undermine the effectiveness and integrity of the system in practice: in general, procedures should be reviewed to ensure that they adequately address procedures in the case of system failure.

Further, at the time of writing, we have not yet received a procedures manual for Presiding Officers (POs). While we understand that such a manual is being drafted, its absence is potentially a significant control weakness. Additionally, it limits the scope of the work carried out by us to date.

Throughout this document, based on the work we carried out, we identify a number of risks which, in our opinion, exist in the system as proposed. We also suggest in each case a number of procedures which could be implemented to mitigate these risks. In some cases, it may be possible to introduce such additional procedures in advance of polling. In other cases, it may be more difficult to conclude whether the continuing existence of the remaining risks identified is compatible with the secrecy and, particularly, the accuracy of voting.

An overarching, general concern in the context of the EMS as proposed is the level of discretion afforded returning officers (ROs). Under the current system (and previous manual voting systems), ROs are responsible for ensuring the integrity of the voting and the counting of the votes. Under a manual voting system, this role was performed in a context which was publicly visible (e.g. through the checking that ballot boxes were empty at the opening of voting, the physical existence of a paper ballot, the public nature of the count) and where an audit trail existed. Hence, significant public oversight of the process was possible.

The proposed electronic voting system fundamentally alters the relationship between the voter, the RO and the vote. The RO sets up the system, oversees its implementation and also reviews his/her own work in satisfying him/herself regarding the integrity of the process. This breaches a fundamental principle of effective controls, i.e. segregation of duties[1]. This risk was mitigated under a paper ballot system as there was transparency in the process (e.g. through the public oversight of the physical count, etc.) and an audit trail which could subsequently be used to assess the accuracy of the result. The proposed electronic voting system is not characterised by these mitigating factors to the same extent. We recommend that the process of setting up and implementing the system and returning the election results be re-examined with a view to introducing adequate segregation of duties.

As noted above, such a segregation of duties is largely absent in the system proposed. In our opinion, it is a fundamental characteristic of good control procedures and for the reasons outlined is increasingly important in the context of the proposed voting system.

In our opinion, a voter, independently or publicly verifiable audit trail is the most effective means of assuring the accuracy of voting, as it would add transparency and provide an audit trail for subsequent verification of the result. Under the proposed system, transparency and auditability have been sacrificed for secrecy. On that basis, while the level of secrecy of ballot may be quite high (with certain exceptions associated with the potential use of technology), the accuracy of the system is more difficult to assess. If there is potential that the EMS components can be undermined through, for example, tampering, controls procedures such as those recommended here may serve to prevent or detect such tampering.

## Introduction

The CoEV has been charged with reporting on the secrecy and accuracy of the Powervote/Nedap electronic voting and counting system.

We have been requested by the CoEV to review the significant control procedures of the EMS with a view to highlighting key risk factors and reporting to the Commission on the extent to which these risk factors can be mitigated by existing or additional control mechanisms. The scope of this element of the work excludes IT processing controls. Our report assumes that the software, machinery, PCs and other computer-related resources have been tested and verified as operating as intended and primarily assesses non-IT controls which could potentially prevent error and/or tampering.

### Scope of our Review

As described in our tender document and set out below, we reviewed the significant control

[1] This is not a commentary on the integrity or otherwise of ROs but introduces a fundamental characteristic of good controls to provide assurance regarding the accuracy of the voting system. It would also serve to provide protection for ROs in demonstrating the efficacy of the process in cases where the vote is challenged.

procedures of the EMS with a view to highlighting key risk factors and reporting to the Commission on the extent to which these risk factors can be mitigated by existing or additional control mechanisms. The scope of this element of the work excluded IT processing controls.

For the purposes of our review, we based our work on documentation provided by the Commission and the DoEHLG and discussions with the Assistant Principal (Franchise) at the DoEHLG. On that basis, our review comprised:

- A risk assessment identifying key control risks arising in the context of the EMS outlined,
- Evaluation of the ability of existing control procedures to mitigate identified risks,
- Recommendations for improved control procedures where necessary, and/or
- Suggestions for further actions available to the Commission.

The scope of the work outlined above depended on the level of access to relevant documentation available to us. The work outlined here is a review of the design of the controls over the system. It is not a formal audit and therefore cannot verify the actual results derived from the system, which will also depend on the proper implementation of the procedures and the effectiveness of the controls over data processing.

**Methodology**

During the course of our work, we reviewed the following documents:

- Memorandum for the Guidance of Constituency Returning Officers at the European Parliament Elections 11 June 2004 - received 24 March 2004;
- Memorandum for the Guidance of Returning Officers at the Local Elections, June 2004 - received 24 March 2004;
- Memorandum for the European Local Returning Officers at the European Parliament and Local Elections, 11 June 2004 - received 24 March 2004;
- Security and Audit Features of the Election Management System, January 2004 - received 29 March 2004; and
- Powervote Electronic Voting and Counting System Manual - received 29 March 2004.

We also interviewed Assistant Principal (Franchise), DoEHLG at his offices on 2 April 2004 and had further discussions with him by phone on 19 April with a view to gaining a further understanding of the procedures proposed in this context.

## Assessment of Risk and Controls

In our opinion, the most effective basis on which to establish the accuracy of the ballot is by way of a voter verified paper audit trail ('VVAT') and the implementation of effective control procedures surrounding the EMS. On that basis, in the absence of a VVAT, the approach adopted by us in the course of our work is to review the adequacy of the input and output controls surrounding the electronic voting management system.

Further, in the absence of a VVAT, a strong control environment is even more important in assuring the integrity of the process. In addition, while the software may be secure, if the controls surrounding the process are not, there may be opportunity for error and fraud.

A new voting system gives rise to new risks and therefore a necessity for new controls and for adapting existing control procedures. In particular, the process of electronic voting involves new modalities of storage, transport, processing and counting of votes, potentially requiring the replacement of existing controls and procedures with new controls and procedures which take account of the new voting environment.

**Responsibility of Returning Officers**

It is our understanding that the individual ROs are each ultimately responsible for the polls in their areas. The DoEHLG does not issue binding instructions to the ROs in relation to the conduct of the polls, though guidelines are issued.

In the overall context of the election process, ROs are responsible and accountable for the conduct of the polling and the counting and returning of votes. The resulting level of discretion afforded to ROs limits the scope of our work as the procedures reviewed are expressed as guidelines rather than being required procedures. This limits the extent to which the procedures can be relied upon to have effect in practice.

Furthermore, the procedures as set out in the documents reviewed by us as part of our work suggest that ROs are responsible for setting up the system, overseeing its implementation, reviewing their own work and the work of others. In the EMS, control is effectively vested in one person, the RO. That person controls the process and also performs several self-checking functions. Effectively, this means that, on an ongoing/real-time basis, the ROs are required to satisfy only themselves as to the accuracy of their own work. It is only in the event of a court challenge that the RO is required to account for the conduct of the election. This would include producing all supporting documentation, which is held for a period of 6 months by the RO, after which it can be destroyed.

The separation of the individual who performs a function from the individual who authorises/approves/checks that performance is central to the principle of segregation of duties. Consistent with best practice, therefore, we would expect to see many more control procedures at each step of the process (such as approvals, checking and review of documentation, restrictions on access to information, etc.).

If there is significant risk of human error (which may be high where there is unfamiliarity with a new system) or if a person responsible for a particular function abuses that responsibility, this cannot be adequately addressed in a situation where there is inappropriate segregation of duties and limited reporting responsibilities.

**Recommendation:**

- We recommend the segregation of the various duties associated with the electoral process. These functions may be characterised in three parts:

1. the set up of the voting machines (including the programming of ballot modules etc.) until their despatch to polling locations;
2. the running of the election, including ensuring the integrity of the voting machines and the efficient running of the voting on election day; and
3. the counting of votes and the returning of the election results.

- Consistent with best practice in the context of control procedures, we recommend that these three functions be carried out by three different persons acting independently of each other under the oversight of the appropriate RO(s). As set out in the Powervote Manual (p. 4 of the section dealing with the local level), functions 1 and 2 are carried out at the service level (the ELRO) while function 3 is carried out at local and constituency level. We recommend a further segregation of the duties noted under 1 and 2. For example, the individual(s) programming the module should not be the individual(s) reading it in to the system. In this instance, the RO remains responsible for the overall management of the election and the returning of the results but delegates key functions to separate members of staff. The RO then has an oversight function to ensure that the duties in question are carried out correctly.

- The guidelines for ECROs, ELROs and LROs outline a number of requirements, while other requirements have been mentioned to us verbally, for which we have not seen documentary evidence. We recommend that the ROs be requested to maintain full documentation of all the forms and reconciliations to be completed, as well as of the main decisions they have made in relation to the conduct of the election. We further recommend that a review process take place after the election to help streamline the process across constituencies and enhance consistency in the process in future elections.

**Use of an updated version of the IES software**

We understand that a new version of the IES software has recently been approved for use on polling day. This may be detrimental to public confidence in the process and represents additional risks in a number of areas:

- As all EMS components have already been delivered nationwide, a process of installing the software nationwide will have to be undertaken. There is a risk that the software used in the election will be inconsistent across constituencies.
- Any testing previously carried out on the software may no longer be valid as a result of changes made to the software.

**Recommendations:**

- We recommend that strict controls over the installation process be implemented. Clear responsibilities for the installation should be assigned and a confirmation procedure (such as both software engineer and RO signing off on installation for each electoral area, including a checklist to ensure completeness in installation) should be implemented.

- We recommend that testing of the new software be carried out on a representative sample basis across the country after the installation process is complete. This testing on a sample basis should be documented and any exceptions should result in an expansion of the sample of software tested.

- Once testing has been completed satisfactorily, we recommend that strict controls, such as those we suggest in this document, be enforced over access to PCs with the software.

**Variations in the competency of staff across polling places**

Both the Guidance for the European Constituency Returning Officer (ECRO) and the Returning

Officer (ELRO) emphasise the importance of having staff that are competent in the use of the electronic management system. Although commendable, the definition of "competent" appears to be left up to the ECRO and the ELRO. As a result, several issues arise particularly in the case of an introduction of a new voting system such as that envisaged.

Across polling places there may be wide disparities in the technical abilities of the on-site staff. Problems that were easily handled by one site may be handled differently or even mishandled by another site. Voters in the latter sites could feel (or actually be) disenfranchised. Additionally, this would be damaging for perceptions of the validity of the electronic process.

As mentioned on page 230, ELROs already possess sole discretion in many areas. Given the importance of technical performance in this election, endowing the ELRO with complete control over the technical elements of the election can reduce the perceived validity of the process. This is especially true if there are close or disputed results, or technical failures. Allocating the technical competence decision to the ECRO alone (with ELRO oversight) may be helpful and provide additional segregation of duties. An allied problem is how the ECRO or the ELRO determine competence.

How any staff member is to obtain this competence is not specified. While we understand that training of electoral staff is underway, the same training of all staff members should be required. If such training is not cost-effective for all staff members, the DoEHLG could define specific areas of competence, with corresponding measures or evidence of such competence.

**Recommendation:**

- We recommend that the DoEHLG define "competence". If possible, consistent training courses, materials or procedures should be offered. Further, the potential conflict (or overlap) between the duties of the ECRO and the RO in terms of determining the competence of their staff should be resolved.

**Opportunities for the generation of a paper trail**

As discussed above, the absence of a VVAT makes any opportunity for hard copy verification that much more important for demonstrating a controlled environment. Several times during the programming of the ballot module the current instructions describe a print option for the results of programming steps. In no case, is it required. In each case it is a simple (one-button) choice to make. Subject to the integrity of the software, it would provide good evidence to verify the crucial programming task.

**Recommendation:**

- A hard copy printout of the results of each stage of the programming task should be made whenever the system allows. These printouts should form part of the documentation to be maintained by the ROs, as discussed in the recommendations regarding the responsibility of ROs.

**Controls over EMS components before polling**

**Key Risk 1: The EMS components (VMs, PCs, PRUs, modules, IES) delivered are not of the**

**same specification ordered. Therefore, the hardware and software on the machines are not that which was tested and approved.**

The DoEHLG has approved and commissioned a particular functional specification from Nedap, the EMS providers. While the DoEHLG is entitled to rely on the vendor to properly supply the commissioned components, there are documented cases where the software supplied in electronic voting systems was not that approved. Therefore a risk exists, and the DoEHLG needs to satisfy itself that the components delivered are as specified.

**Recommendation:**

- To mitigate this risk, we recommend additional checking by the DoEHLG on a representative sample basis to confirm that the specification of the components delivered, in particular, the software conforms to that ordered. We also recommend the documentation of this sample-based confirmation.

**Key Risk 2: The EMS components are physically damaged on delivery to the storage facility or are damaged or tampered with during storage.**

EMS components were held in a storage facility before distribution to the ROs. Safeguards should have been in place to ensure that there were sufficient quality control checks on the EMS components delivered, suitable storage conditions to prevent damage and stringent access controls to the storage facility to prevent tampering. These safeguards should have included restricting access to all but essential staff, security clearance measures, and maintenance of a record of all personnel accessing the relevant storage area. Assurance that the machines were not damaged or tampered with during this period depends on whether these measures were in place and witnessed by DoEHLG.

**Recommendations:**

- The CoEV should obtain documentary confirmation from the DoEHLG that the appropriate safeguards were in place and operated effectively throughout the storage period.

- We understand from discussions with DoEHLG staff that they are currently planning visits by DoEHLG staff and *Nedap* engineers in May 2004 to all ROs to check all voting machines, software set-up & programming etc. This provides additional assurance that malfunctioning software/hardware will be identified before the election and corrective action taken. We endorse such an approach and recommend that the DoEHLG report to the Commission on the outcome of this exercise.

**Key Risk 3: The EMS components are lost, damaged, replaced or tampered with while in the custody of the ROs before the election.**

a) **Risk arising from inadequate records of EMS components**
b) **Risk arising from unsuitable storage of EMS components**
c) **Risk arising from inadequate security over EMS components**
d) **Risk arising from inappropriate storage arrangements of EMS components between elections and the timing of issue of the EMS components**

*(a) Record of EMS components*

The delivery of EMS components to ROs commenced in September 2003 and most of the components are already in the possession of the relevant RO. 28 European Local Returning Officers (ELROs) have received software, voting machines, programming/reading units, ballot modules, PCs and CDs. 114 Local Returning Officers (LROs) and 4 European Constituency Returning Officers (ECROs) have received software, PCs and CDs.

We understand that Nedap has maintained a written record of the serial number of each IES, VM, PC, PRU, module and details of the RO to which each component was issued and that a copy of this record is maintained by the DoEHLG.

**Recommendation:**

- We recommend that the DoEHLG also maintain records of the CDs issued. This would reduce the risk of invalid CDs being introduced to the election process. Consistent with best practice with respect to segregation of duties, we also recommend subsequent reconciliation of components issued and returned by a DoEHLG staff member other than the staff member handling the issue of components.

*(b) Suitable Storage*

There is a risk that EMS components will be damaged and fail to operate as intended if stored in unsuitable conditions. To prevent damage, it is essential that ROs are made aware of the importance of considering the storage requirements and the suitability of proposed storage facilities (in particular, that locations previously used to store ballot boxes may be inappropriate for a voting machine). We note that there are storage guidelines for the voting machine included in the Powervote manual.

The risk of failing to detect damage to a component is mitigated because the components have a self-checking mechanism when initially booted which produces an error message if there are failures.

**Recommendation:**

- We recommend that further reference to the importance of proper storage for all EMS components be made in the various memoranda for the guidance of ROs, including guidelines as to what constitutes ‘proper’ storage. Adherence to these guidelines should also be clearly documented.

*(c) Secure Storage*

There is a risk that unauthorised access is obtained to EMS components (while in the possession of the ROs), which are then tampered with and fail to operate as intended. We believe this prospect to be a significant risk because it will be more difficult to detect as efforts will have been made to conceal such tampering. While several preventative measures have been taken, such as disabling of USB ports, floppy drives, etc., to minimise the risk, we have not identified specific instructions to ROs concerning either the importance of, or the requirements for, secure storage to prevent unauthorised access to EMS components. It is possible that ROs, more familiar with the paper-based system, are not aware of the potential for tampering and may incorrectly believe that the components cannot be tampered with without detection. Therefore, they may not be cognisant of their role in the security process.

**Recommendation:**

- We recommend that specific guidelines are issued to ROs and referenced in the memoranda for the guidance of ROs, highlighting the importance of secure storage of all EMS components. This should include a requirement to (1) evaluate the security access issues in their particular location; (2) instigate stringent controls over access to all EMS components to prevent unauthorised access; (3) document who will have access to the components and (4) satisfy themselves as to the extent of their adherence to the issued guidelines. We further recommend that access by an individual to any EMS component should only be permitted in the presence of the RO and that access by any other individual should be restricted to the minimum necessary for the performance of the ROs duties. The RO should also maintain a written log of those who have had access to any EMS component.

**Security of Ballot Module**

Modification of the ballot module has the most serious consequences, because it contains the original record of the vote. If alterations have been made to components used subsequent to polling, such as the count PCs or CDs, the original module and backup module will still contain the original record of the vote. However, if the programming of the ballot module has been tampered with, or the module replaced, the voting record will be compromised. Therefore, particularly rigorous safeguards need to be maintained over ballot modules.

The risk that the programmed ballot module is tampered with or replaced following insertion into the voting machine, and that this is not detected, can be mitigated by several controls. The general controls outlined above for all EMS components, such as the written record of serial numbers issued and the prevention of unauthorised access, should apply to ballot modules. Additionally, once the ELRO inserts the programmed ballot module into the voting machine, s/he secures the machine with three plastic numbered seals – one around the centre of the machine, a second at the back of the machine and a third around the metal flap securing the ballot module. We have not yet ascertained the extent to which the seals in question can be replicated, which represents an additional risk. However, assuming the seals cannot be replicated, once the seals are broken they cannot be re-sealed.

The sealing of the module provides assurance that the ballot modules programmed by the ROs are those in the machines on election day. It is important that sealing occurs directly after programming to minimise the opportunity for tampering with the ballot modules. The PO at each polling station will confirm the status of the seals before the opening of polls, add the seal numbers to the VM1 form and certify on that form that each seal is intact.

We understand from discussions with DoEHLG staff that the keys to each voting machine are common to all voting machines, and therefore we do not consider these an effective control mechanism.

If an individual did succeed in replacing both the ballot module and the seal, then it is only when the ballot module is read in at the read-in centre that the tampering could be identified. However, at that stage, the only recourse available is to render the poll invalid. Therefore, controls to prevent tampering before polling are particularly important.

**Recommendations:**

- We recommend that a document noting the seal number and signed by the RO should be delivered to the PO independently of the voting machine. The PO should check the number as indicated by the RO on the document to the seal on the ballot module. This would provide additional assurance that the ballot module has not been tampered with following insertion into the machine.

- We also recommend that POs be issued with written guidelines concerning procedures to be followed if the seal on the metal flap of the ballot module is not intact or if the seal number does not correspond to the number on the written document. Specifically, we recommend that these procedures involve the non-use of the machine in the event that the seal on the ballot module is broken, as there could be no assurance of integrity for the data derived from a module for which the security procedures have been breached. We recommend that the PO should return the original seals with the VM1 form to the RO, who checks the seal number to the original list of seal numbers. The RO thus verifies that the original seals were present on the machine before polling commenced.

- We understand from our discussions with DoEHLG staff that ROs have been advised to programme spare modules for the election, to prepare for failure of a machine at a polling station. (Current estimates suggest up to 30 machines may fail during the election). While it is appropriate that these measures are taken, safeguards in the form of records of the issue and use of spare modules should be maintained by both the RO and the DoEHLG. ROs should provide a written account - independently countersigned - of the use of spare modules as well as any spare modules that were not programmed. They should also certify at the end of the election that they have physically accounted for all spare modules issued to them. In this manner, assurance can be given that spare modules have not been misused during the election process.

*(d) Storage between elections*

We consider that an essential safeguard of EMS components is the central storage of all components at a secure location between elections. This reduces the risk of tampering between elections.

**Recommendations:**

- Following each election, the components should be recalled by the DoEHLG, independently reconciled to the written record to ensure all components are returned by the appropriate RO, and held in secure storage until the next election. This would reduce the risk that an individual obtains access to a component, becomes familiar with its operation and devises a method of tampering. While we appreciate that central storage is an additional cost, we believe it to be a necessary one.

- Prior to the next election, the same procedures surrounding issue of components should apply. Additionally, machines should be tested before they are issued, in order to reduce as far as possible the potential for errors after delivery to the local areas.

- We understand that it has been procedure in the past that ballot boxes were maintained by the ROs between elections. This was a practical and sensible approach, but is inappropriate to the new system. In the paper system, while the ballot box had been stored by the RO before the election, on polling day it was generally easy to show that the ballot box had not been tampered with and was empty. The Powervote manual states that there are self-checking mechanisms built into the software, which ensure that "everything is functioning correctly". However, the 'open poll statement' print-out, showing that no votes have been recorded on the module, is the only control mentioned that the machine operator can monitor. There is no indication given as to how an error message would appear or how a machine operator should react to such a message. We do not believe that this is a sufficient control to confirm that the machine or module have not been tampered with, as in the absence of physical controls over the machine and ballot modules between elections, it is possible that they could be interfered with. Further, the form of this interference may not necessarily be pre-recorded votes. For example, the module could be programmed to give votes to one candidate when the voter casts a preference for another candidate. This alteration would not be identified by the printout showing no votes at opening of the poll, and is thus not as effective a control as the viewing of an empty ballot box.

**Timing of issue of EMS components**

Issue of the EMS components to ROs significantly in advance of polling day decreases storage costs, facilitates early identification of faults and provides an opportunity for the RO to become familiar with the various components. However, we consider that issue of the components so far in advance of polling unnecessarily heightens the risk of tampering.

**Recommendation:**

- We recommend that EMS components are issued to ROs shortly before the final date for nominations. If ROs are given adequate training in the operation of the components, opportunity to operate them in a training setting, and components are tested before issue, then it would only be necessary to issue the component a short time in advance of the final date for nominations, so that installation of IES can take place. While we acknowledge the practical difficulties associated with this recommendation, we believe that such a measure would significantly reduce the potential for tampering with the EMS components.

**Key Risk 4: Errors occur during the various stages of the voting process, including the set-up of the ballot modules and voting machines, for which there are no procedures to handle such errors.**

A general limitation of the documentation relating to the EMS system is that the instructions provided do not specify what should be done if any of the steps in the process or components fail, or even if an error message will be displayed. For example, if the ballot module at set-up is not "verified" what will be displayed or is such a failure even possible? We understand that there are a substantial number of possible error messages which could arise in relation to EMS components. While it might be considered impractical to make operators aware of all such error messages, we believe the most common and/or likely error messages should be documented.

An Incident Report exists, for which no reference is made in any manual, and could be used to document errors.

**Recommendation:**

- We understand that the DoEHLG is instigating a help desk which will be available during polling and counting to assist in solving any problems or difficulties arising. We consider this step to be a sensible one, but believe that it would operate more efficiently if the most common problems and solutions to such problems were documented and explained to the operators in advance of polling.

**Key Risk 5: Procedures to test the voting buttons during the set-up of the voting machines are incomplete such that a vote cast may not be recorded correctly or recorded at all.**

The buttons on the voting machine are tested before and after the ballot papers are positioned on the voters' panel. In both instances, however, the current instructions state that only <u>one</u> button be pressed to make sure that the buttons are functional, that the ones programmed to accept a vote are correctly identified, and that the ones that are not programmed to accept a vote are correctly disengaged. In each case, the assumption is made that if one button in each category is correct then all of the other buttons in that category are similarly correct.

This is a risky assumption. From a physical perspective, faulty hardware could disable an individual button. With the current instructions, this situation could only be detected, during polling, by an observant voter. Unless the "observant voter" was the first voter to press the faulty button, votes would be lost until the problem was discovered. If it were not detected during polling, it would be detected after polling when vote totals did not match. This would be too late.

Software could also be tampered with to disable a candidate's button or, to redirect a vote for one candidate to another. In the former case, the voter's preference could be displayed on the voter panel, convincing the voter of its authenticity, but then the vote would not be counted. The latter situation would not even be detected by other procedures after polling is complete because all of the counts would match.

A complete testing of all of the buttons would be a one-time task. The lack of procedures for the failure of a button was already mentioned in Key Risk 4. One possibility in the case of a failure of a button is to replace that voting machine with a spare and re-start the initiation process.

**Recommendation:**

- All buttons on the voting machine must be tested prior to and after inserting the ballot papers. The results of this step should be documented and sent with the materials, after polling, to the read-in/count centre. Procedures for handling button failure should be documented.

**Key Risk 6: The election details are set up incorrectly on IES by the RO and subsequent vote recording is inaccurate.**

**Ballot paper preparation and insertion**

The LROs and ECROs are responsible for the input of candidate data into IES and the preparation of ballot papers for their electoral area. It is possible that they make an error and the incorrect ballot paper is printed and inserted into the voting machine. It is also possible that a falsified ballot paper is inserted into the voting machine, although this risk is mitigated by the presence of security seals on the machine.

The risk of incorrect input of candidate data by the LRO or ECRO and the subsequent printing of an incorrect ballot paper is mitigated by the fact that candidates or their agents may review the ballot paper prior to printing and could identify in advance if the ballot paper is incorrect. Additionally, it would not be difficult to rectify such error in advance of polling day.

The current instructions for inserting the ballot papers in the voters' panel refer to positions that are "determined in the earlier stages of preparation". We understand that the DoEHLG determines, as far as possible, the column order of the ballot papers. However, incorrect insertion of the ballot papers at local level could lead to erroneous results.

**Recommendations:**

- We recommend that to further ensure that the ballot paper on the voting machine has not been tampered with and replaced, the PO should be furnished with a separate copy of the ballot papers – highlighting the column order in which they should appear – along with the other documentation sent to him by the RO on the morning of the election, and should confirm on the VM1 form that the ballot paper on the voting machine corresponds to the ballot paper issued by the RO.

- Procedures detailing how the ballot paper position information is transferred to the insertion step should be identified and verified. We recommend that the arrangement for candidates or their agents to view the ballot paper be formalised to ensure independent verification of the insertion of the ballot paper.

**Service Level**

The ELROs are responsible for the set-up of the election details, insertion of polling stations, import of the ballot papers and then programming of the ballot modules. It is likely that they will be assisted by their staff, including local authority IT personnel. However, there does not appear to be any independent check on the election set-up and subsequent ballot module programming. Therefore, we believe that there is a risk of election details being set up incorrectly and that this is not identified.

**Recommendation:**

- This risk would be best addressed by a segregation of duties as outlined in the executive summary, such that the RO would review rather than input and review the set up of the election on IES. For the forthcoming election, we recommend that details of the election set-up are reviewed by an individual other than the person who inputs to the IES.

**Risks arising during polling**

**Key Risk 7: Lack of a manual for presiding officers.**

We understand that a manual for POs is currently being drafted but have not yet had sight of or received such a manual. This is a significant limitation to the scope of our work as a manual for POs appropriate to the context of electronic voting constitutes a significant element and description of the control environment. The recommendations outlined here should be considered for inclusion in a final version of a manual for POs (and may already be under consideration in that regard).

**Recommendation:**

- We recommend that a manual detailing all appropriate procedures to be followed by POs – including any modifications to their tasks as a result of this report – is completed and circulated to POs in good time for the election. The manual should address in detail the procedures to be followed by POs in the course of their duties as well as in the case of system problems or failure.

**Key Risk 8: A voting machine failure during polling is dealt with inappropriately**.

According to statistics quoted in the memorandum for the guidance of ELROs, 0.5% of voting machines may fail. This amounts to 30 out of approximately 6,050 in use on election day. There are some procedures in place for this event, including the set-up of a help-desk, staffed by Nedap engineers and software designers, and DoEHLG staff, which will be available throughout polling day for all election staff. However, there are inadequate documented procedures regarding actions to be taken by polling station staff in the event of a breakdown. Therefore, there is a risk that a breakdown is dealt with inappropriately and questions subsequently arise as to the integrity of the data on the ballot module taken from this machine.

**Recommendation:**

- It is essential that written guidelines are issued to polling staff outlining specific procedures to be instigated in the case of a failure of a machine. These guidelines should include reference to who should remove the ballot module, who should witness the removal, and sign-off from the witnesses regarding proper treatment of the module. There should also be a clear requirement for the same procedures to be followed in the case of the use of a new machine and new module as were applied to the original machine at the opening of polling (print out of open poll statement, etc.).

**Key Risk 9: There is a risk that voters will misunderstand how the process of casting their votes works and that as a result, they will be prevented from exercising their constitutional right to vote at any or all of the elections.**

With the new electronic system, there may be some confusion as to what exactly the procedure is for casting the vote. For example, a voter completes his/her preference selection for the local election and then casts the vote, thinking that each election is separate and therefore should be cast separately. While a warning is given on the voting machine display unit, individual voters may not be cognisant of this.

**Recommendation:**

- We understand from discussions with DoEHLG staff that road shows will take place nation-wide and that a substantial advertising campaign is planned for the period prior to the polling day. In addition, posters setting out clearly the cast vote process will be visible en-route to and inside the polling station (including one in the direct vicinity of the polling machine and visible to the voter at the machine). Two voting machines set up with a mock election will be included as part of each road show to guide voters through the process and to highlight important elements of the process (such as the warning regarding elections for which preferences have not yet been indicated). We strongly endorse this exercise and consider it essential to mitigate the risk of voter misunderstanding and disenfranchisement.

**Key Risk 10: There is a risk that if voters are allowed to vote at machines other than the one designated for their area, that this will negatively impact on the important control procedure of being able to reconcile voter tickets issued to votes cast.**

Voters, on presenting at the polling station, are marked off the electoral register and provided with a voter ticket. This ticket corresponds in number with the number of the machine designated for their area. This ticket is handed to the polling officer on duty at each machine. We have been informed that, in particularly busy periods, voters may be directed to other voting machines in the same polling building to cast their votes. A significant existing control is that a reconciliation between tickets issued and votes cast is carried out for each machine: this provides assurance that all and only votes cast are recorded in the machine. We understand that this reconciliation could also be carried out for each polling building. While we acknowledge that this is a pragmatic approach to reducing delays in the voting process, we believe the approach represents additional risks to the voting process as noted below.

**Recommendations:**

- We recommend that voters should only cast their vote at the voting machine designated for their use. A building-wide reconciliation would only be possible after the poll has ended, whereas it may be necessary to carry out an immediate reconciliation of a particular voting machine during polling (e.g., to reconcile votes cast where a machine has malfunctioned during polling). Additionally, the potential for delay between the issue of a voter ticket and voting poses an additional risk that voters who are issued tickets do not vote. This undermines the reconciliation of tickets to votes. Therefore, we recommend that, should large queues form at a particular machine, voter tickets should not be issued until the resulting delays have abated. We appreciate that this will not alleviate delays during busy periods, but believe the additional risks to the integrity of the voting process outweigh the practical benefits of reducing waiting time.

- This recommendation should be included in the procedures manual for POs.

- The risk of queues developing could be minimised by a well-publicised campaign encouraging voting at off-peak times.

**Risks arising after polling**

**Key Risk 11: The ballot modules could be misplaced, tampered with, or replaced after the close of poll and before delivery to the read-in centre.**

If modules may be replicated technologically, this constitutes a significant risk. However, the consideration of such an IT risk is outside the scope of our work.

In the context of our review of the control procedures, we understand that the following procedures are in place:

- A close of poll statement is printed off, detailing valid votes cast, null votes and deactivations. This statement is to be dated, timed and witnessed.
- The close-poll function immobilises the ballot module so that no new votes can be recorded.
- VM1 (Polling Station Reconciliation Form), and VM2 (Opening and Closing Statements where printer is not working) forms are required to be completed by the PO. The module, VM forms, marked register, ticket booklets and voting machine seals are to be delivered to the read-in centre by hand in an envelope.
- Modules have unique identification numbers stored electronically and printed onto the outer casing.
- A minimum of two people will be charged with the delivery of the module to the read-in/count centre.

The read-in/count centre could be a significant distance from the polling station, which could lead to a number of problems:

- The module could be misplaced or tampered with en-route to the read-in centre.
- If individuals charged with delivery of the module also have access to the modules and the formatting of modules process, prior to the poll, they could have prepared modules on which they have carried out a fictitious vote.

**Recommendations:**

- We recommend that the ballot modules are not enclosed with the VM forms, etc., in an envelope, but are secured separately in a special container, which is sealed in a similar manner to the polling machines prior to delivery to the POs.
- We understand that a formal check of the number of valid votes cast, null votes and number of deactivations of the polling machine (taken from the close of poll printed statement and/or form VM1) is reconciled with the information read into the PC at the read-in centre. We strongly recommend this approach, as this would ensure that any module inappropriately introduced to the process would have to be 100% accurate and would thus significantly reduce the risk of tampering after the close of poll.

- While the IES system will automatically check the module number on read-in, it appears that it would still be possible to introduce a new/different module directly before commencing read-in. Therefore, we recommend that a formal check be carried out of the module numbers (on the outer casing of the module) returned for read-in, to ensure that the number(s) submitted for read-in is/are either
  - the same number that was delivered with the polling station machine and recorded by the RO, or
  - can be reconciled to recorded polling machine breakdowns (for which new machines/modules are to be used).

  Consistent with segregation of duties, this check should be carried out by an official/RO independent of the official issuing ballot modules.

- The above recommendations should be included in written guidelines provided to all ROs.

**Key Risk 12: The CD upon which the votes are burned could be over-written or replaced en-route from the read-in centre to the count centre (which may or may not be in the same building).**

The delivery of the information from the read-in centre to the count centre via CD is, in our opinion, a stage of the process that is very susceptible to potential tampering with the result of any individual election and thus represents a significant risk after the close of poll. Our conclusion is based on a number of key factors:

- Tampering with the CD does not require specialised equipment. CD drives and writing facilities are standard on most modern laptop computers.
- Tampering with the CD does not require significant specialist knowledge.
- Unlike the ballot modules, CDs are a standard form of information storage and are readily available.
- Invalid CDs could easily be concealed.

We acknowledge that the above risks could be somewhat mitigated by the fact that the original record of the poll is held at the read-in centre (see our specific recommendation below in respect of this).

These risks are particularly significant in relation to the European elections due to the delay between read-in of the polling module on Friday, 11 June 2004 and the count on Sunday, 13 June 2004, given the time frame in which tampering could take place.

**Recommendations:**

- We recommend that steps be taken to ensure that the CDs used in the election process are particular to the election, individually identifiable and not easily replicated. We recommend that all CDs to be used in the process be issued directly by the DoEHLG with a departmental insignia stamped on each. This stamp could include a unique ID number, which would enable a record of all CDs issued and used to be kept and checked. We understand from discussions with DoEHLG staff that they are currently consulting with the Local Government Computer Services Board concerning supply of CDs, which will incorporate such features.

- We recommend that before transferring the CD to the count centre, the ELRO signs the outside of the CD, and that only CDs originally signed are accepted at the count centre.

- We recommend that steps be taken to ensure the security of the information on the CD. Such steps could include using read-only CDs and the use of password protection on the files, of which only the RO at the read-in centre and the RO at the count centre are informed. We understand from discussions with DoEHLG staff that they currently intend to use CD-Recordables rather than CD-Rewritables and we consider this a worthwhile security measure.

- We recommend that, prior to the result being announced, the RO at the count centre and the read-in centre confirm data such as number of valid votes cast. This procedure may detect evidence of tampering with the CD en-route to the count centre.

- In relation to the European elections, as well as the above recommendations, we recommend that the polling module numbers are reconciled as described in the previous recommendation regarding the physical security of the modules. These CDs should be sealed in a container similar to the manner in which the polling machines were sealed and stored in a secure location (e.g. a Garda station) until they are read into the PCs on Sunday, 13 June 2004.

- Inappropriate access to the CDs in advance of counting may undermine the secrecy of the vote before counting. The implementation of the above procedures would also mitigate against such risks. For similar reasons, we recommend that stringent security measures are implemented over the PCs at the read-in centres after the CDs have been despatched, since the PCs will continue to hold the data from the modules read in. These measures should be documented in specific guidelines issued to ELROs.

**Key Risk 13: The PCs and PRUs used in the read-in and count centres could be tampered with prior to and during the read-in/counting process.**

The EMS process requires the use of in excess of 500 PCs nationwide. By tampering with the PCs and PRUs, individuals could affect the counting of ballots, as the processing of the ballot information would be corrupted. Control procedures currently in existence to reduce the risk of tampering include the use of hardened PCs and password protected access to PCs.

**Recommendation:**

- We recommend that procedures be issued to ROs specifically outlining effective security procedures and access restrictions, including continuous supervision of the EMS components at the read-in and count centre.