28

Achieving an Integrated Design: The Way Forward for Information Security

Jean Hitchings, University of Nottingham, ICL Institute of Information Technology, Nottingham, NG7 2RD. email: jean.hitchings@nott.ac.uk

Abstract

For some time it has been suggested in literature that information security is not just a technology problem, but that it also concerns people (Hitchings, 1994). Information systems and their associated controls are designed by people. The integrity of such systems rely on the designers knowledge of potential problems. It is also dependent on users adhering to security procedures. In addition, there is always someone with a high level of control in any system. This person could be someone authorized to transfer large sums of money or it could be a systems administrator with the highest level of privilege on the information system.

This research develops a new methodology to information security design which has a totally different approach because it does not just consider the technical factors of an information system. Other factors, such as the human issue should be equally important when designing an information system where a main component will be people. This paper proposes a new methodology which includes human and contextual issues as well as technical solutions.

Methodologies should be regarded as a tool and used as a catalyst to analyze and design good information systems. This tool can be adapted so that it fits the organisation or application system under study. In this sense a methodology can therefore be regarded as a virtual tool that although has its basis in a defined framework, it can be changed to suit the needs of every application or organisation. This is what happens in practice. A good example is Structured Systems Analysis and Design Method (SSADM) which was developed by the Civil Service and is used in many types of Government organisations. Each version of SSADM has been slightly altered in order to adapt to the new organisation. Downs, Clare and Coe (1992) state that 'although earlier versions of SSADM were adaptable some people never wanted to hear that message, or apply it! Version 4 of SSADM's modularity stresses the fact that it needs to be adapted to the needs of each project.'

The methodology that is proposed in this research is therefore a framework that can be adapted by organisations in order to reveal the major information security issues of the organisation. It has been named the Virtual Methodology because it roots only are concrete and solid. The framework consists of models, which are constructed in a manner appropriate to the organisation and application system under consideration. The methodology should be able to change and evolve as it encounters new problems or types of application systems.

J. H. P. Eloff et al. (eds.), *Information Security — the Next Decade*

1. OUTLINE OF THE VIRTUAL METHODOLOGY

The Virtual Methodology (VM) does not just concentrate on technical aspects but also incorporates some of the features of the soft systems methodology (SSM), such as, organisational, contextual and human issues. However, VM differs from SSM (Checkland,1981 and Checkland and Scholes,1990) because it studies not just the organisation that runs the information system but also the environment within which the organisation operates. For example, factors such as legislation are also considered.

Another major difference is that the aim of VM is to implement not an information system but the security for an information system. SSM was designed for solving information system problems. It considers all aspects of the information system including the people, the organisation and the associated culture. SSM then attempts to draw models of the problem situation. These models are used as a basis of discussion between interested parties. When one model has been agreed to be the most appropriate, desirable changes are designed and implemented.

VM begins by constructing models of the organisation. Each model will include details about the environment, for example, it could include relevant details about competitors. The people issue is considered along with their cultures and how they interact not only within the organisation but also with outsiders, such as customers or suppliers. So VM analyzes the organisation in context with its environment. In addition, the information system is analyzed in context with the organisation. In both models there is an emphasis on the interactions that take place, for example, between one employee and another, or between an employee and the information system.

When an organisation model and an information system model have been agreed, a model of risks is constructed. The risks model is created by combining the organisational and information system models. The types of controls required can then be determined.

Until now VM has only been concerned with conceptual issues, this allows for changes to be made easily at a later stage. If precise physical details were designed early on in the analysis phase, a small change later could have radical repercussions. This is in line with current systems analysis thinking.

The next step is to design controls, this is necessarily concerned with physical issues. This stage demonstrates another difference between VM and other methodologies because it advocates that the designer should also consider the possibility of developing new tools, should appropriate ones not exist. The proposed information security is implemented and regularly reviewed and maintained.

Below is a summary of the Virtual Methodology phases:

Analyze the organisation;
Analyze the system in context to the organisation and personnel involved;
Analyze the system and determine risk areas;
Analyze the system and determine the types of controls that are required;
Design controls;
Implement the system;
Regularly review and maintain the system.

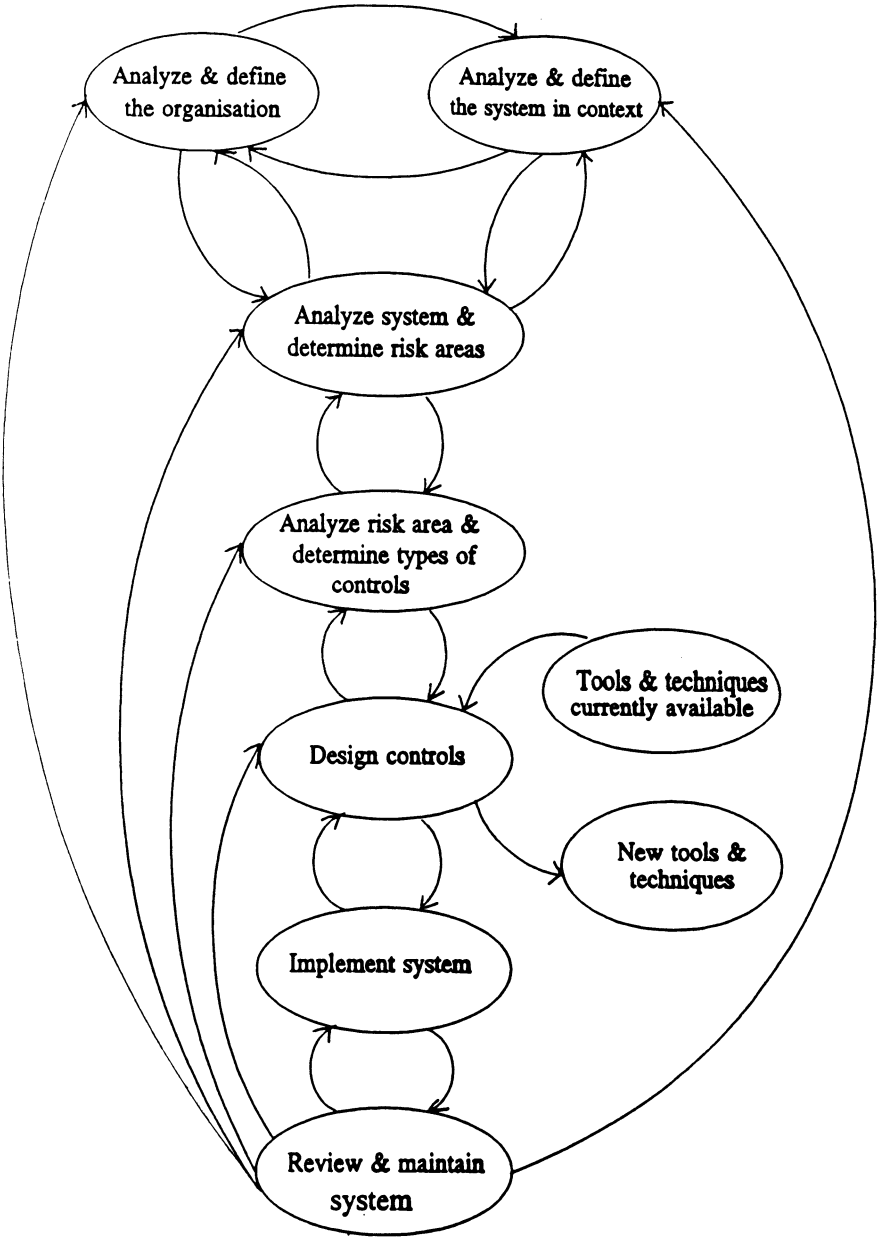
These phases are illustrated in figure 1 where it can be seen that they do not necessarily have to be undertaken in a set sequence. For example, the application system can be analyzed before the organisation, or current tools and techniques could be looked at first. Note that system in this methodology refers to the application system under study. The diagram also shows that each stage interacts with others and that the entire process is iterative. Discussions from one stage may cause designers to return to a previous stage.

2. AIM OF THE VIRTUAL METHODOLOGY

The aim of the Virtual Methodology is to assist in developing security at an adequate level for a particular information system. The security recommendations should be appropriate to the functions of the application system and should consider the contextual, organisational and human aspects. As previously stated the contextual, organisational and human issues are rarely taken into account when information system security is designed, and in many cases no consideration is given to them.

The main problem is that the information system is used by people and it is up to these users as to how well they adhere to policies. Disgruntled users may ultimately cause the system to fail. The human issue is therefore a vital component. Major changes should be negotiated with appropriate personnel. The organisational issue is important because it creates the environment in which the information system is going to run. The environment outside the company should also be considered as the organisation does not conduct its business in isolation.

Figure 1 Outline of the Virtual Methodology phases



3. THE PHASES OF THE VIRTUAL METHODOLOGY

3.1. Introduction

Because of the importance of contextual, human and organisational aspects, the first phase includes a study of the organisation in context. The results of this are then channelled through all subsequent phases. The objective of the first phase is to produce an organisational model which describes the structure and philosophy of the company as well as its functions. Interactions are very important and must be represented in this model.

The model must also include other aspects such as the boundaries of the organisation. This is not a simple matter as often outsiders, for example customers, can influence decision making within the organisation, possibly by choosing or not choosing a particular product. For example, the current trend in consumer purchasing is for green products which is forcing companies to change the type of goods they sell.

What must also be considered is the influence that the organisation has on the rest of society, such as customers and competitors. If no company is prepared to manufacture green products then customers do not have the opportunity to buy them. However, if one organisation starts to manufacture them, then consumers may opt to buy that brand. If this is done in large enough numbers then other companies will be encouraged to offer similar products.

In addition, some large companies are able to influence smaller companies directly. For example, IBM. Many small companies standardise on IBM compatible products and follow the large company as it evolves. By doing this they are able to gain more custom. Therefore the organisation can have an impact on its competitors, and equally its competitors can have an impact on it.

The second phase analyses the information system in context with the findings from the first phase. It also considers the personnel involved who need not only be employees. The output from this phase is an information system model showing the interactions that occur, for example, a user accessing the system.

The third phase combines the organisational and information system models in order to create a model of risk areas. Interactions are the main feature of this model. The fourth phase analyzes the risk areas to determine what types of controls are needed, for example, if the information system was networked there must be some network access controls.

The fifth phase is where specific controls are designed for each risk area. At this point cost/benefit analysis and constraints are considered and the suggested controls are implemented. It is not until this phase that any physical factors should be considered. The reason for this is that it is much easier to alter a system at a conceptual level, before it has become set and entrenched in factors other than design issues.

The final phase is to regularly review and maintain the existing system. Although these phases are numbered they do not have to be carried out in this order, and as the phases interact it may be desirable to return to ideas from previous stages and discuss them. Therefore this methodology should be considered as a fluid process where discussions can ebb and flow from one phase to another.

3.2. Phase 1: Analysis of the organisation

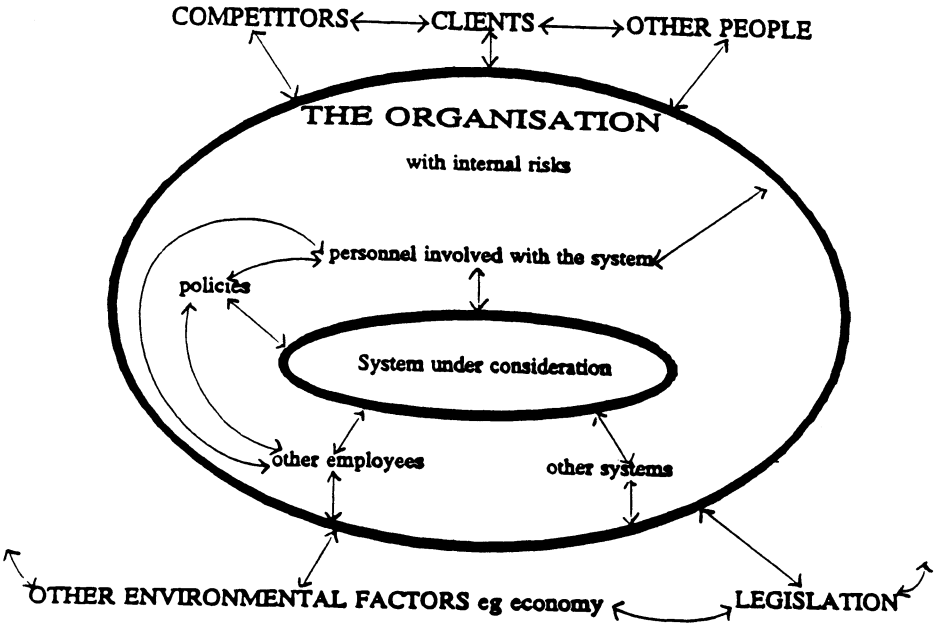
When analysing an information system it is helpful to create a model which shows an overview of the system. This high level view can then remind the analyst what the entire information system is like. This is particularly useful when concentrating on specific aspects of the system. The model shown in figure 2 assists the analyst to concentrate on the factors which interact with not only the application system but also the organisation, the policies and the personnel. Note, there is no box around the environment, this is intended to give the analyst the feeling that firstly the environment is not finite and secondly to remind the analyst that there could be other factors that have not yet been considered.

Systems analysis has traditionally been undertaken by data processing personnel who often have a technical approach to design and may not consider other relevant aspects. In addition, if this technical person is to design controls, they may be designed on logic, rather than looking at the information system with an open mind and considering other ways that the system could be breached. This highlights the need for a number of people to analyze the system. Checkland (1981) and Checkland and Scholes (1990), explain that each person has a different *Weltanschauungen*, or view of the world. This is echoed in many works on systems, for example, Wilson (1984) and Davis and Leddington (1991), where it is thought that a better perception of the problem situation can be obtained by combining and discussing different viewpoints.

Originally, only the technical aspects of a system were considered, and it was analyzed as if it exhibited rational and logical behaviour. Personnel and organisational issues are areas that were considered in the same vein, if they were considered at all. It should be clear that personnel are not logical and rational and therefore a new way of analysing systems is required. Checkland (1981) and Checkland and Scholes (1990) have suggested a basis for this new approach with Soft Systems Methodology (SSM).

SSM includes some subjective perspectives, this is good because it allows for natural curiosity, exploration of the situation and promotes discussion. This is opposed to objective perspectives that are narrow in approach, and where early assumptions tend to become fixed throughout the development, and discussion and exploration tend to be very limited. The implementation aspects of SSM tends to be weak, but this is improving as can be seen from Checkland's more recent work (1990). The VM methodology utilises some of the soft system approach because it engenders discussion and considers human and contextual issues.

Figure 2 Virtual Methodology model of the organisation



In constructing a model of the organisation all aspects should be considered. The more people involved in designing the model, the more chance there is of obtaining an accurate representation of the entities that make up the organisation and their interactions.

The organisation is a huge, complex and dynamic structure with a network of interactions and relationships. The best the analyst can achieve at this stage is a snap shot of what is happening at that moment. This can be used as a building block, so that in later stages this will continually be reviewed and reconsidered as it evolves.

The initial stage in building a virtual model would be to consider the components that make up the organisation, for example they could include, the applications systems, the personnel and the policies. Next the analyst can add the environmental factors that surround the organisation, for example, clients, competitors and legislation. Consideration must be made of the relationships between such factors and these can be shown by thin black lines, with arrows depicting the flow of information. Relationships that should never occur should be shown as thick black lines; and those that should occur under certain situations depicted by dashed lines.

This model should then be discussed with other people, including users, who will have their own idea of the organisation, and eventually an agreed model should evolve. Each arrow will highlight where the possible risks may occur.

3.3. Phase 2: Analysis of the system

In phase 2 a model is constructed showing the information system in context. Interactions are an important part of this model and will include not only those within the information system, but also how the information system interacts with the rest of its environment.

Users can be identified and arrows drawn to indicate the type of access they should be allowed. For example, an arrow pointing from the system to the user indicates that the user only receives output, either by screen displays or reports. These outputs can be requested by the user. An arrow pointing both to the user and the system indicates that the user can update and enter data as well as obtain reports. Finally, the last class of user is one with a dashed arrow from the system to the user, which shows that the user can access the system under certain controlled situations, such as data processing personnel accessing the live system. Figure 3 summarises the types of access and Figure 4 shows an example of a Virtual Methodology model of an information system.

Figure 3 Types of access to the system

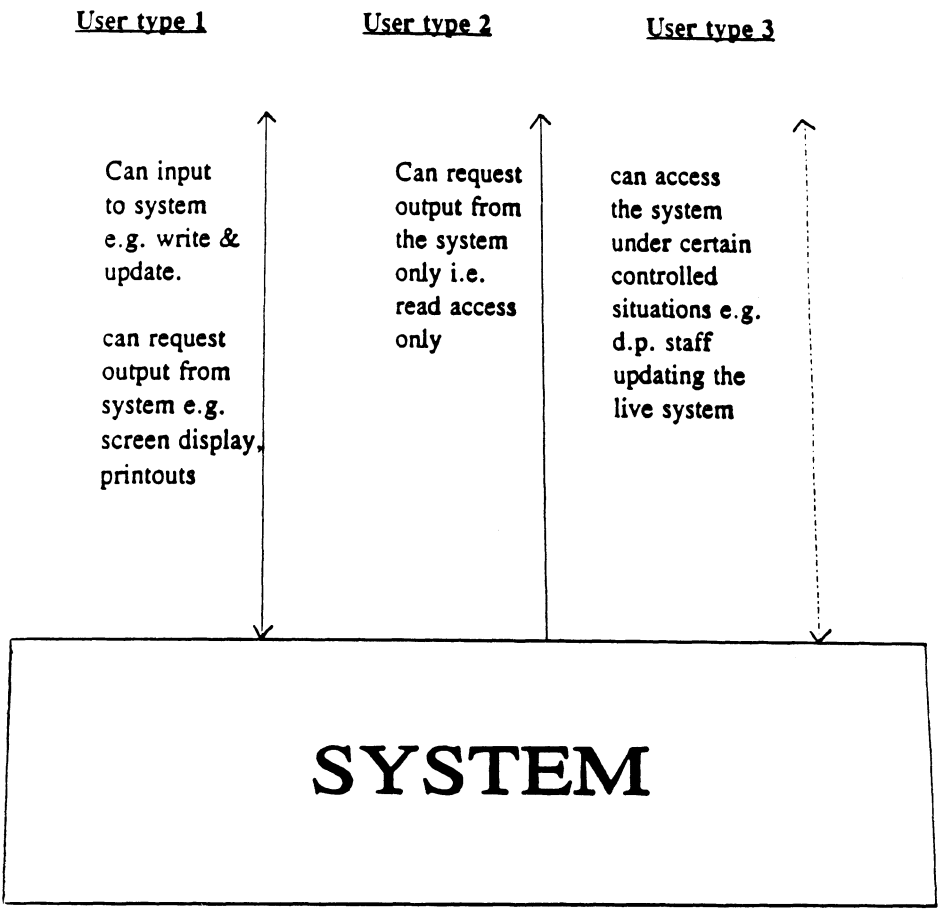
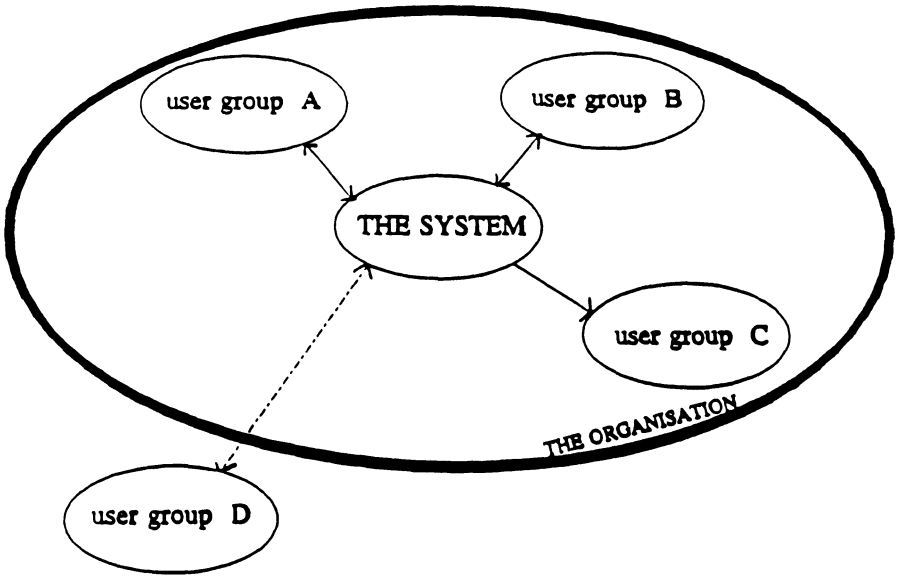


Figure 4 VM model of a system

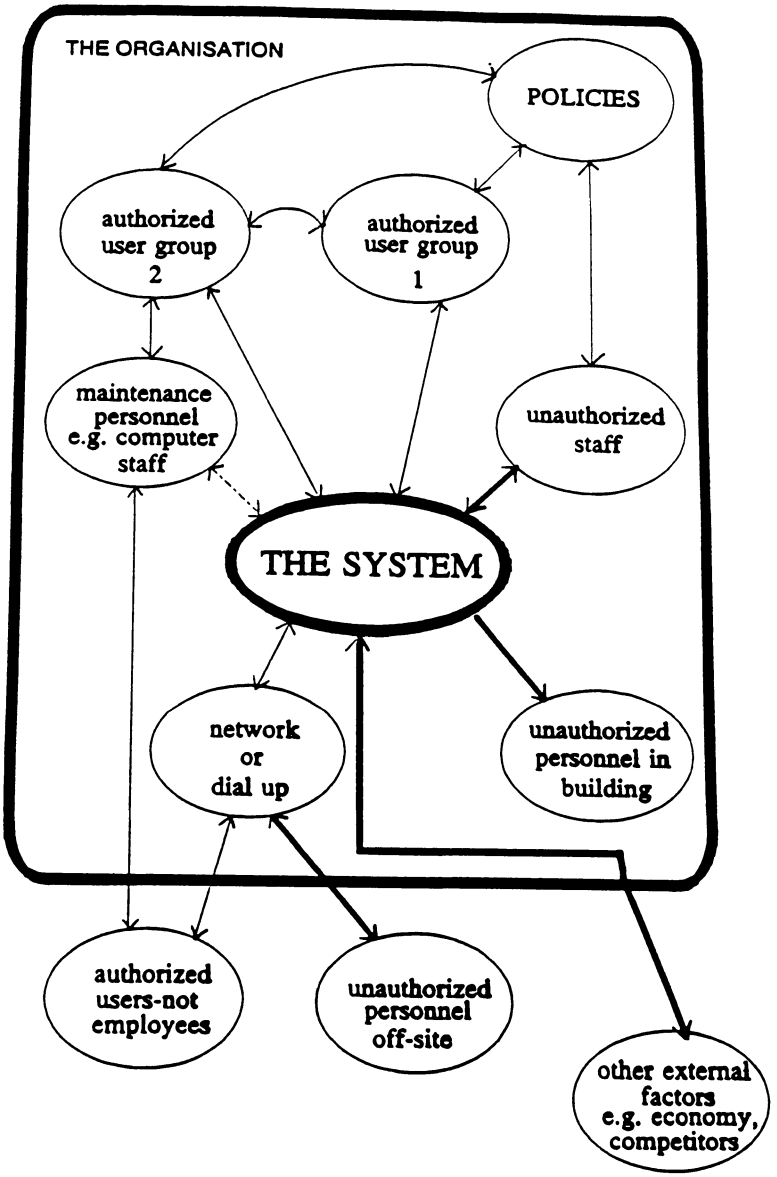


3.4. Phase 3: Analysis of the system to determine risk areas

This stage combines phases 1 and 2, and by considering the interactions (arrows) between the information system and its environment and it is possible to produce the Virtual Methodology risk model. It is important to consider both the organisational and system models, as for example, policies can create an environment which is conducive to breaches in information security. A policy of allowing staff to load their own programs to play games during the lunch time will create an environment which could allow information systems to be infected by a virus program.

It is also important to define the boundaries within which information security restrictions can be imposed; however for risks emanating from outside, the organisation can only recommend security procedures. Figure 5 is an example of a Virtual Methodology model of risks.

Figure 5 VM model of risks



3.5. Phase 4: Analysis of risk areas to determine the types of controls required

In this stage the risk areas are analyzed in context to the organisation and environment, for example, personnel, competitors and legislation. The types of controls required can then be identified. From figure 5 the following risk areas may be identified:

1. Data and programs are an obvious risk area and these should be protected using logical and physical access controls.
2. Networked systems have an additional security need. Access should be restricted to authorized personnel by using network access controls.
3. People are a problem and access to the information system must be restricted to authorized users only. This means that other employees or members of the public should not be able to gain access. This should include logical access controls to the information system as well as physical access controls to the site, room and equipment.
4. An organisation cannot implement all the necessary controls suggested in 3 above if the users are not their own employees. For example good password management can only be suggested to external users but management have no authority to implement it.
5. Maintenance personnel are a special type of user as they are allowed to access the live system under certain controlled situations. Access should not be granted to such personnel unless special procedures are followed. Logical and physical access controls as well as special procedures, such as monitoring or supervision, are required.
6. Incorrect policies can be a problem and therefore all policies should be regularly reviewed once they have been implemented.
7. Collusion between staff is a risk area and traditional managerial controls should be implemented, for example, separation of duties.
8. Collusion between staff and outsiders is an additional problem. Again management controls should be implemented and working conditions and pay should be satisfactory.

3.6. Phase 5: Design controls

In this phase the conceptual controls are transposed into actual controls.These must be found from existing tools or techniques or they may have to be specially designed. Cost benefit analysis must be undertaken before any controls are implemented.

Continuing with the previous example, the following controls could be adopted providing they are financially feasible.

Risk area from phase 4	**Controls that may be implemented**
1	Logical controls could include: program authorization e.g. RACF; and database management controls. Physical protection to restrict access to the rooms or equipment could include locks (traditional or combination), Tan cards, and tokens. Backups should be taken and stored off site. A backup system should be available if necessary. Good password management is essential. Passwords should be revoked if staff leave or transfer, passwords should be checked to see if they are easy to guess, procedures should be in place to enforce passwords to be changed regularly.
2	Network controls are usually supplied with the network package. These should be implemented.
3	Logical access controls to the system could include, for example, restrictions to allow users to log on from specified terminals only. Logical access control to equipment could include, for example, a personal computer security software package. Physical access controls to the site/ room/ equipment could include, for example, traditional locks, combinations locks and Tan cards. Users should implement good password management. Passwords must be difficult to guess, but easy to remember. Users should change their passwords regularly and not write them down.
4	Suggest controls recommended in 3 above are implemented by the external company/ user.
5	User ids and passwords should only be made available by authorized request from management. These user ids and passwords should be revoked immediately after use. All changes to the live system must be planned, supervised and monitored. Maintenance personnel who require access to the computer room should be escorted and not given keys or codes to the room.
6	All policies should be reviewed and those that put the system at risk should be amended. It should be considered whether additional policies are required.
7	Collusion between employees is a management issue and can be made less likely by adequate supervision and separation of duties. For example, the manager who gives permission for the live system to be updated should not be the manager who supervises the updates.
8	Collusion between employees and outsiders is also a management issue. Good working conditions may help to deter such practice but management must be vigilant particularly of disgruntled employees.

3.7. Phase 6: Implement the system

The controls outlined in phase 5 should all be appropriate and economic and can now be implemented to improve the security of the information system.

3.8. Phase 7: Review and maintain the system

This should be an on going analysis phase that ensures that the system responds to changes in the organisation, the environment, legislation and to include the latest technology and concepts which will provide the organisation with an up to date and appropriately secure system.

4. CONCLUSION

The Virtual Methodology begins by considering an overall picture of the organisation and its environment. It then looks at the application system and the risk areas. The types of controls are discussed at a conceptual level and it is not until the final design phase that physical aspects of the system are discussed. Each phase consists of debates including as many interested parties as possible. By including users it may highlight problem areas in implementing controls, for example, some procedures may be too time consuming. Lyytinen and Klein (1985) state that peoples behaviour is based on their view of the world which is another reason for user involvement.

The deliverables are in a format that can be understood by management, users and technical computer personnel. The models are representations of the components that are considered relevant to the organisation and the system, including the interactions between each component. The lists of risks and types of controls are kept at a conceptual level and are in an easy to understand form. The final list consists of recommendations of actual tools and techniques that could be implemented. Each suggestion should again be discussed and evaluated to see if it is feasible both from the economical point of view as well as the practical aspects of implementing the new procedures.

VM has been designed to be applied to any information system within any type of organisation. The final phase of VM is to continually evaluate and enhance the system and therefore it should evolve with the organisation reflecting any new changes that may occur. It is a dynamic methodology incorporating contextual, organisational and human issues with technical solutions, and leads the way forward in information system security design.

5. REFERENCES

Checkland, P. (1981), *'Systems thinking, systems practice'*, Chichester: Wiley.

Checkland, P. and Scholes, J. (1990), *'Soft systems methodology in action'*, Chichester: Wiley.

Davis, L. and Leddington, P. (1991), *'Information in action, soft systems methodology'*, Basingstoke: Macmillan Education Ltd.

Downs, E., Clare, P. and Coe, I. (1992), *'Structured systems analysis and design method application and context'*, Hemel Hempstead: Prentice Hall International (UK) Ltd.

Hitchings, J. (1994) 'The need for a new approach to information security', *Proceedings of the Tenth International Security Conference IFIP SEC '94*, Curacao, 23 - 27 May 1994, Elsevier North Holland.

Lyytinen, K. and Klein, H.K. (1985), 'Information systems epistemology: an historical perspective', *Research methods in information systems*, ed Mumford, Hirschheim, Fitzgerald and Wood-Harper, Amsterdam: North Holland.

Wilson, B. (1984), *'Systems: concepts, methodologies and applications'*, Chichester: John Wiley and Sons.