A Prototype for Assessing Information Technology Risks in Health Care

E. Smith[1] and J.H.P. Eloff[2]

Rand Afrikaans University, Department of Computer Science
PO Box 524
Auckland Park 2006
Republic of South Africa
Email: [1]elme@pixie.co.za
[2]eloff@rkw.rau.ac.za

Abstract

Although a vast number of risk-management methodologies have been proposed thus far and even though these methodologies are being applied to all types of organizations quite effectively, a few concerns are raised when the self-same risk-management methodologies are applied to the health-care environment. The authors, therefore, developed a risk-management methodology, entitled "Risk Management in Health Care – using cognitive fuzzy techniques" (RiMaHCoF), that is specifically tailored for the health-care environment. The methodology comprises five successive stages in all, namely initiation, domain analysis, risk assessment, risk analysis and domain monitoring. In the present paper, however, the authors will focus only on the third stage, viz. the risk assessment stage.

This paper is principally aimed at expounding a prototype for the risk assessment stage, which prototype will incorporate cognitive fuzzy-logic techniques — as opposed to conventional techniques, such as annual-loss exposure (ALE) calculation — by means of which to assess the information-technology risks potentially to be incurred in the health-care domain. In this way, it will be ensured that human common sense and intuition (which form the basis of any risk assessment exercise) will not be omitted from the risk management process.

Keywords: cognitive fuzzy-logic techniques, fuzzy logic, health care, information technology risk value, risk assessment, risk management methodology

Introduction

Information technology is currently being employed in healthcare environments across the globe, resulting in significant improvements in the efficiency and quality of all services rendered in this realm. The prospect of storing healthcare information in electronic form does, however, raise concerns about the risks that could be incurred upon exposing highly confidential and sensitive healthcare information to outsiders [1-35]. The occurrence of a risk, such as the unavailability of patient information owing to a power failure, could compromise not only the patient's privacy, but also quite literally his/her wellbeing. It is imperative, therefore, to be able to identify possible risks in good time and to implement the necessary countermeasures in order to protect the patient in the healthcare institution.

Broadly speaking, the term 'risk management' can be defined as 'that process by means of which to identify and implement countermeasures that will, at best, prevent risks from occurring and, at worst, minimize their effect if they were to occur' [36-38]. A number of powerful techniques (such as CRAMM) could be employed to facilitate the prevention and/or management of potential information technology risks [39, 40]. healthcare information systems are, however, quite unique when compared to other information systems, with the result that they require a different approach to risk management [41].

For this reason, the authors developed a risk-management methodology, entitled "Risk Management in Health Care – using cognitive fuzzy techniques" (RiMaHCoF), that is specifically tailored for the healthcare environment [42]. The purpose of a healthcare institution is to take care of its patients, with the result that the patient should be the primary concern of these institutions. To incur a risk (such as unauthorized access to patient

ELSEVIER ADVANCED TECHNOLOGY

Computers & Security
Vol 21, No 3, pp000-000, 2002

0167-4048/02US$22.00

information) in this environment could compromise not only the *patient's privacy*, but also quite literally his/her *well-being*.

Just as important as the need to protect the patient's privacy is the need timely to *share* accurate patient information in order to ensure its availability to all authorized parties and, in this way, to ensure the proper treatment of the patient. In order to accomplish the sharing of patient information in an atmosphere of trust, any trusted organization or person could be appointed to act as trusted adjudicator between the various authorized communicating partners. Sensitive patient information could then be shared via the trusted authority, as well as protected against unauthorized access. The dilemma of obtaining, using and sharing patient information to provide care whilst not breaching patient privacy is a serious concern. Security controls implemented to minimize risks must, therefore, be evaluated in terms of their functional abilities to protect the privacy of the patient, as well as to provide accurate and timely information to all authorized parties.

The electronic patient record contains various *sub-classes* of patient information, such as the personal information of the patient, like the patient's name, address and telephone number, and financial information, such as the amount due for a specific consultation. These sub-classes of patient information are *distributed* between the various authorized communicating partners, such as the doctor, pharmacy and hospital. Each authorized communicating partner could, therefore, gain access to a specific sub-class (or sub-classes) of the information contained in the electronic patient record. This very distributed nature of the electronic patient record, however, increases the number of possible risks that could be incurred, owing to the fact that there are many communicating partners, of whom some could be untrustworthy. Threats will also continue to evolve together with overall technological developments in IT and networking.

Most of the consequences of incurred risks in the healthcare domain are extremely difficult to quantify, owing to their *non-monetary* nature. It is, for example, extremely difficult to determine the cost associated with the incorrect diagnosis and treatment of a patient owing to inaccurate patient information. Furthermore, some part of the patient information, such as the clinical information, could be considered confidential, whereas another part thereof, such as the geographical information, could well be considered unclassified. The latter introduces a certain degree of *vagueness* regarding the decision-making process with respect to securing patient information.

Another concern regarding the vulnerabilities of a healthcare institution is its being subjected to *unique exposures*, such as medical professional liability, managed-care errors and dealing with emergency situations that differ greatly from those in other enterprises. If a patient were, for example, admitted to the casualty unit of a hospital, it would be essential for the patient information to be made available at once in order to properly treat him or her. In this scenario, the unavailability of patient information could quite literally lead to loss of life. Many of the vulnerabilities that threaten healthcare information systems are, in fact, a matter of *life and death*, and should, therefore, be protected through security controls.

Finally, it is oft-times difficult, if not impossible, to isolate the assets of the healthcare system from the traffic flow of patients, their visitors and doctors. This has introduced even more threats to the healthcare system and has created an urgent need to protect patients' privacy.

The RiMaHCoF methodology accommodates these unique features of the healthcare environment.

The proposed IT risk management model focuses on the technical aspects of securing patient information. Human aspects, such as keeping passwords confidential and changing

Jan Eloff has been a Professor in Computer Science at the Rand Afrikaans University since 1988. He received a Ph.D. (Computer Science) from the Rand Afrikaans University. He gained practical experience by working as a computer management consultant specializing in the field of information security. He is chairman of the Special Interest Group in Information Security (affiliated to the Computer Society of South Africa, IEEE). He is also chairman of the International Working Group 11.2 of IFIP specializing in small systems security. He delivered papers at leading information security conferences on an international level. He is an evaluated researcher from the Foundation for Research Development (FRD), South Africa. He advises to industry on various information security projects. Contact him at the Computer Science Department, C-ring 521, Kingsway, Auckland Park, RAU, South Africa; eloff@rkw.rau.ac.za.

passwords frequently, are not the primary focus of the model.

The scope of the proposed IT risk management model is defined in terms of its *Information Technology (IT)* and *Information Security (IS)* components. The scope of the model is first defined in terms of the IT domain it addresses. The proposed risk management model focuses specifically on IT risks; in other words, on those risks that pose a threat to the IT used to store, process and disseminate patient information in a healthcare institution. The IT scope of the risk management model is, therefore, limited to the IT used to store, process and disseminate patient information, such as a database, microfilm and a local area network.

The scope of the proposed risk management model is also defined in terms of the Information Security (IS) it provides. IS can be defined in terms of the five security services rendered under it, namely identification and authentication, authorization, confidentiality, integrity and non-repudiation. The primary aim of any healthcare institution is and should be to treat its patients. An IT risk management model designed specifically for this domain must, therefore, protect the patients and their healthcare information in order to ensure their proper treatment. The proposed risk management model will, for this reason, address IS specifically by focusing on the *confidentiality* of patient information. It is important to note, however, that the remaining IS services, namely that of identification and authentication, authorization, integrity and non-repudiation, also play an important role in securing patient information. Further research should, therefore, be conducted into these.

The methodology (as depicted in Figure 1) comprises five successive stages in all, namely initiation, domain analysis, risk assessment, risk analysis and domain monitoring. This paper, however, will be devoted to a closer look at the third stage only, viz. the risk-assessment stage.

The principal aim of this paper is to expound a prototype through which to implement the risk assessment stage of the RiMaHCoF methodology. The prototype thus expounded will incorporate human common sense and intuition (which form the basis of any risk assessment exercise) by following a cognitive fuzzy-logic approach to the assessment of information technology risks that might be incurred in the healthcare environment. The prototype will also serve to identify the high-risk areas in a typical healthcare institution.

The first section of the paper will be devoted to an overview of the risk assessment stage of RiMaHCoF as implemented by the prototype.

Figure 1: A graphic representation of the various stages in the RiMaCHoF risk management methodology for a typical healthcare institution.

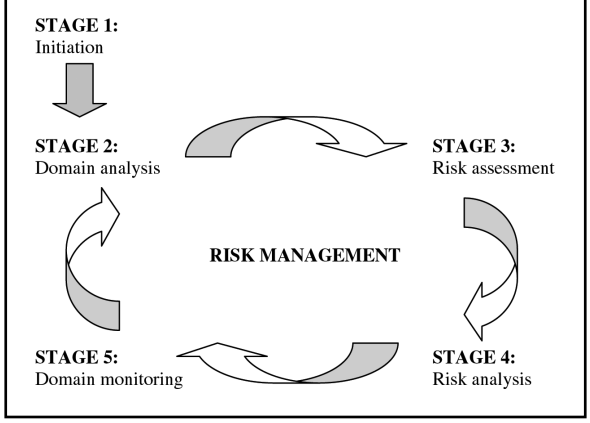
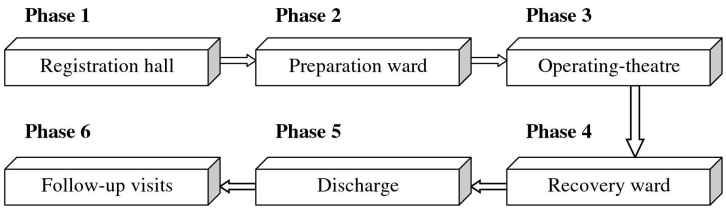


Figure 2: Route followed by a patient admitted to hospital for an operation.



In this way, a clear picture will be obtained of the purpose and deliverables of the prototype. The latter part of the paper will be devoted to an in-depth discussion of the prototype itself.

An overview of the risk assessment stage of RiMaHCoF

The principal aim of any healthcare institution is to treat its patients. When a patient pays a visit to a healthcare institution, he/she could follow various routes through such institution, depending on the purpose of his/her visit. An example of the route followed by a typical patient admitted to hospital for an operation is depicted in Figure 2.

Each *patient route* consists of a finite number of *phases*. The hypothetical patient route depicted in Figure 2 consists of six phases, namely phases effected in the registration hall, the preparation ward, the operating theatre and the recovery ward. The last two phases to be effected would be the discharge and follow-up visits phases. A 'phase' constitutes the treatment received and the time spent in a specific division along a specified patient route.

Risk assessment for the healthcare environment is aimed at identifying high-risk patient routes (i.e., *critical* patient routes) in a typical healthcare institution with a view to enhancing the information security of such institution. This process is best explained by means of an example.

Supposing we need to identify the critical patient routes for a typical hospital. Three critical patient routes would then be identified, *viz.* the route a typical patient would follow to have X-rays taken, the route a typical patient would follow upon admission to the casualty unit and the route a typical patient would follow when admitted for an operation. As was mentioned before, each of these routes consists of a finite number of phases. The first patient route (to have X-rays taken) would entail phases effected in the registration hall, the waiting ward and the X-ray room. The second patient route (that route followed upon admission to the casualty unit of the hospital) would entail that treatment be received and/or time be spent in the registration hall and the casualty unit, as well as that time be spent during the treatment and release phases (if we proceeded on the assumption that the patient's condition was such that he/she could be treated immediately, without, for example, having to have X-rays taken or be operated on). Finally, the last patient route (when admitted to hospital for an operation) would consist of five phases, during which the patient would have to receive treatment and/or spend time in the registration hall, the preparation ward, the operating theatre and the recovery ward, as well as the discharge and follow-up visits phases (as depicted in Figure 2).

In order to determine which of these routes should be deemed critical, the high-risk phases (the *critical* phase) in each patient route need to be identified first. This involves determining an information technology risk value for each phase to be effected along a specific patient route. Such information technology risk value is based on the information technology domain a typical patient will be exposed to during a specific phase along the patient route he/she is following. If, for example, the IT risk values for the phases effected in the registration hall, the waiting ward and the X-ray room were calculated as 340, 865 and 220 respectively, the waiting-ward phase would be the only phase along this patient route that, to a scale of 0 to 1000, could be considered critical (owing to its high IT risk value).

Having calculated such IT risk value for each phase along a specific patient route, these values are consolidated for each route in order to obtain one IT risk value for the specific patient route in its entirety. In this way, all patient routes with high IT risk values can be classified as *critical patient routes*. If, for instance, the IT risk values of the three patient routes in

Table 1: Example of the dynamic components in each phase of the route a typical patient would follow upon admission to hospital for an operation.

	DYNAMIC COMPONENTS		
PHASE	***Technologies***	***Countermeasures***	***Other***
Registration	⇒ Paper files ⇒ Database files	◊ Passwords	• Time spent in phase • Communicating parties sharing patient information • Risk of patient information being exploited
Preparation ward	⇒ Paper files ⇒ Database files	◊ Passwords ◊ Access-control matrix	• Time spent in phase • Communicating parties sharing patient information • Risk of patient information being exploited
Operating-theatre			• Time spent in phase • Communicating parties sharing patient information • Risk of patient information being exploited
Recovery ward	⇒ Paper files ⇒ Database files ⇒ Microfilm ⇒ Local-area network	◊ Access-control matrix ◊ Symmetric encryption	• Time spent in phase • Communicating parties sharing patient information • Risk of patient information being exploited
Discharge	⇒ Microfilm		• Time spent in phase • Communicating parties sharing patient information • Risk of patient information being exploited
Follow-up visits			• Time spent in phase • Communicating parties sharing patient information • Risk of patient information being exploited

our example were calculated as 520, 720 and 888 respectively, then both the route a typical patient would follow when admitted to the casualty unit of the hospital, as well as the route a typical patient would follow when admitted for an operation, would be deemed critical patient routes in this hospital (owing to their high IT risk values). This result would enable the superintendent of the hospital to identify the high-risk areas in the hospital for which countermeasures ought to be implemented in a bid to tighten information security.

The purpose of risk assessment is, therefore, to determine both an *information-technology risk value for each* ***phase*** along a patient route, as well as *an information-technology risk value for each* ***patient route*** in a typical healthcare environment, with a view to enhancing information security in that specific healthcare institution.

Calculating the IT risk value for each phase in a patient route

In the healthcare environment, the information technology domain a typical patient would be exposed to is a *dynamic* one. In a bid more clearly to illustrate this dynamic nature of the healthcare environment, please consider the information-technology domain of a hypothetical patient route, as depicted in Table 1:

Various technologies can be employed in each phase of a patient route to process and store patient information. In the patient route depicted in Figure 2, these technologies might, for instance, include database and paper files in the registration and preparation-ward phases; microfilm, database files, a LAN server and paper files in the recovery-ward phase and microfilm in the discharge phase (as illustrated in Table 1). These technologies are, however, extremely vulnerable to risks. It is, therefore, essential that countermeasures be implemented at best to prevent or, at worst, to minimize the risks that may possibly be incurred.

The technologies employed to process and store patient information and the countermeasures implemented for this purpose are *dynamic* in the sense that both components vary for each phase in a patient route (as illustrated in Table 1). In

addition, the countermeasures can either be upgraded over time or exchanged for new countermeasures. Both the *technologies* and the *countermeasures* are, therefore, examples of dynamic components in a typical healthcare environment.

Furthermore, supposing a typical patient were to spend a certain length of time in each phase of the patient route depicted in Figure 2. During each phase, his/her patient information is, essentially, shared by a number of authorized communicating parties, such as the administrative clerk, the nurses and the doctor. It is, however, also possible that, under certain circumstances (such as an emergency), unauthorized parties might need to access his/her patient information. If a patient were, for example, admitted to the casualty unit of a hospital, the on-duty doctor (who might not necessarily be resident at the hospital the patient normally visits) would need to access the patient's information without delay in order to be able effectively to treat him/her. The inaccessibility of patient information in such case may have dire consequences. The patient information would, for this reason, also be exposed to a number of outsiders, thus increasing the possibility that the confidentiality, integrity or availability of the information might be compromised. The *time spent in each phase*, the *number of communicating parties sharing the patient information* and the *possible risks that might be incurred* are further examples of dynamic components in each phase of the patient route under consideration.

The purpose of risk assessment, as was mentioned before, is firstly to determine an information technology risk value for each phase in a patient route. The authors researched a number of alternative modelling techniques, such as the probabilistic theory, PERT analysis, heuristic modelling and fuzzy logic. The conclusion they had reached was that fuzzy logic techniques present a plausible way of modelling vagueness with respect to quantifying the consequences of IT risks being incurred in the healthcare domain. In addition, it accommodates the vagueness with respect to the decision-making process with respect to securing patient information and it takes full cognisance of human common sense and intuition. Fuzzy logic strikes a balance between human common sense and intuition on the one hand and the manipulation of numbers on the other. The *theory of fuzzy logic* is, however, not discussed in this paper, owing to restrictions as to its length. The reader is referred to [43-44] for more information on this aspect.

A cognitive fuzzy-logic approach, which takes into account all dynamic components in a specific phase, as well as the relationships between these components, is, therefore, followed to calculate such information technology risk value for a specific phase in a patient route. This approach is discussed in more detail later in the paper.

Having calculated the information technology risk value for a specific phase in a patient route, the said phase is classified as a 'low-risk' phase if its IT risk value were to fall between 0 and 350, as a 'medium-risk' phase if its IT risk value were to fall between 351 and 650 or as a 'high-risk' phase, if its IT risk value were to fall between 651 and 1000. The latter classification is based on a numeric scale ranging from 0 to 1000, with 1000 indicating the highest risk value possible. The next step in the risk-assessment process (as implemented by RiMaHCoF) would be to

Table 2: IT risk values for each phase in the route a typical patient would follow when admitted to hospital for an operation.

Phase	IT risk value	IT risk category
Registration	710	HIGH
Preparation ward	515	MEDIUM
Operating-theatre	210	LOW
Recovery ward	856	HIGH
Discharge	360	MEDIUM
Follow-up visits	365	MEDIUM

identify the *critical* (high-risk) *phases* within each patient route.

Consider, for example, Table 2. The 'registration' and the 'recovery-ward' phases have been identified as critical phases in this hypothetical case, because both these phases are classified as high-risk phases according to their respective IT risk values.

Calculating the IT risk value for each patient route in the healthcare institution

Having identified the critical phases in each patient route, the second objective in the risk-assessment stage (as implemented by RiMaHCoF) involves the identification of the critical patient routes in the healthcare institution under consideration. In order to identify such routes, the information technology risk values for all phases in every patient route need to be consolidated. The RiMaHCoF methodology proposes a set of heuristics for consolidating the information technology risk values for all the phases in a specific patient route. These heuristics are summarized in Table 3.

The *theory of heuristics* is, however, not discussed in this paper, owing to the restrictions obtaining to its length. The reader is referred to [45] for more information on this theory.

The aim of consolidating the IT risk values of all phases in a specific patient route is to obtain an overall IT risk value for that patient route. Such risk value could then form the basis for identifying *critical patient routes* in the healthcare institution. In this way, the high-risk areas in the healthcare institution can be pinpointed. This will, in turn, enable management to make informed decisions as to the implementation of countermeasures with a view to enhancing the information security of the healthcare institution.

The classification of a patient route as a 'high-risk', 'medium-risk' or 'low-risk' route is done in the same manner as that of the different phases. In other words, a patient route with an IT risk value between 0 and 350 is classified as a 'low-risk' patient route, a patient route with an IT risk value between 351 and 650 is classified as a 'medium-risk' patient route and a patient route

Table 3: Heuristics as proposed by RiMaHCoF.

Condition	IT risk value of patient route (R_{ROUTE})
Number of critical phases in patient route > 50%	$R_{ROUTE} = \sum_{i=1}^{m} R_i / m$, where m is the number of critical phases in the patient route and R_i is the IT risk value of the i^{th} critical phase in the patient route.
Number of critical phases in patient route = 50%	$R_{ROUTE} = [\sum_{i=1}^{m} R_i / m + \sum_{j=1}^{n} \overline{R}_j / n]/2$, where m is the number of **critical** phases in the patient route n is the number of **non-critical** phases in the patient route R_i is the IT risk value of the i^{th} **critical** phase in the patient route $\overline{R}_j$ is the IT risk value of the j^{th} **non-critical** phase in the patient route.
Number of critical phases in patient route < 50%	$R_{ROUTE} = [\sum_{i=1}^{m} R_i + \sum_{j=1}^{n} \overline{R}_j] / p$, where p is the number of phases in the patient route R_i is the IT risk value of the i^{th} **critical** phase in the patient route $\overline{R}_j$ is the IT risk value of the j^{th} **non-critical** phase in the patient route.

Table 4: Different scenarios with respect to the classification of each phase in the route a typical patient would follow when admitted to hospital for an operation.

Phase	Scenario 1		Scenario 2		Scenario 3	
	IT risk value	Classification	IT risk value	Classification	IT risk value	Classification
Registration hall	710	HIGH	710	HIGH	710	HIGH
Preparation ward	813	HIGH	500	MEDIUM	500	MEDIUM
Operating-theatre	420	MEDIUM	420	MEDIUM	420	MEDIUM
Recovery ward	856	HIGH	856	HIGH	856	HIGH
Discharge	205	LOW	205	LOW	205	LOW
Follow-up visits	660	HIGH	660	HIGH	150	LOW

with an IT risk value between 651 and 1000 is classified as a 'high-risk' patient route. The high-risk patient routes are then identified as the *critical patient routes* in the healthcare institution under consideration.

In order more clearly to illustrate the consolidation of the IT risk values for the phases in a specific patient route, consider the hypothetical scenarios outlined in Table 4.

Consider scenario 1. According to this scenario, there are four critical phases in this patient route, which are effected in the form of visits to the registration hall, the preparation ward and the recovery ward and as follow-up visits. The first heuristic, therefore, obtains, because more than 50% of the phases in the specific patient route (i.e., 4 out of 6) are critical. The IT risk value for the patient route based on this scenario is, therefore, equal to *the average of the IT risk values of the four critical patient routes*, i.e., 760. In this case, the route is, therefore, classified as a 'high-risk' patient route.

Consider scenario 2. According to this scenario, there are three critical phases in the patient route, which phases are effected in the form of time spent in the registration hall and the recovery ward and as follow-up visits. The second heuristic, therefore, obtains, because exactly 50% of the phases in the specific patient route (i.e., 3 out of 6) are critical. The IT risk value for the patient route based on this scenario is, therefore, equal to the *average* of the following: the *average of the IT risk values of all critical phases in this patient route* (i.e., 742) and the *average of the IT risk values of all non-critical phases in this patient route* (i.e., 375). This results in an IT risk value of 556 and the route is classified as a 'medium-risk' patient route.

Finally, consider scenario 3. According to this scenario, there are only two critical phases in the patient route, which phases are effected in the form of visits to the registration hall and the recovery ward. The third heuristic, therefore, obtains, because less than 50% of the phases in the specific patient route (i.e., 2 out of 6) are critical. The IT risk value for the patient route based on this scenario is, therefore, equal to the *average of the IT risk values of all phases in this patient route*, i.e., 474. In this case, the route is, therefore, also classified as a 'medium-risk' patient route.

The identification of critical patient routes in a healthcare institution is used to uncover the high-risk areas in such institutions. In this way, management is presented with a clear picture of the specific patient routes in the healthcare institution that need to be investigated when deciding on the implementation of countermeasures in order to protect the patient in the healthcare institution.

Prototyping the risk assessment stage of RiMaHCoF

Having obtained an overview of the risk assessment stage as proposed by the RiMaHCoF methodology, the prototype can now be

discussed. The prototype is used to achieve the first objective of the risk assessment stage in the RiMaHCoF methodology, namely to calculate an information technology risk value for a specific phase in the patient route in question.

In a bid clearly to illustrate the functioning of the prototype, it is important to use the same example throughout the resultant discussion. The example chosen for this purpose is based on an actual, real-life hospital in South Africa and has proven sufficiently to explain the implementation of the risk assessment stage in the RiMaHCoF methodology.

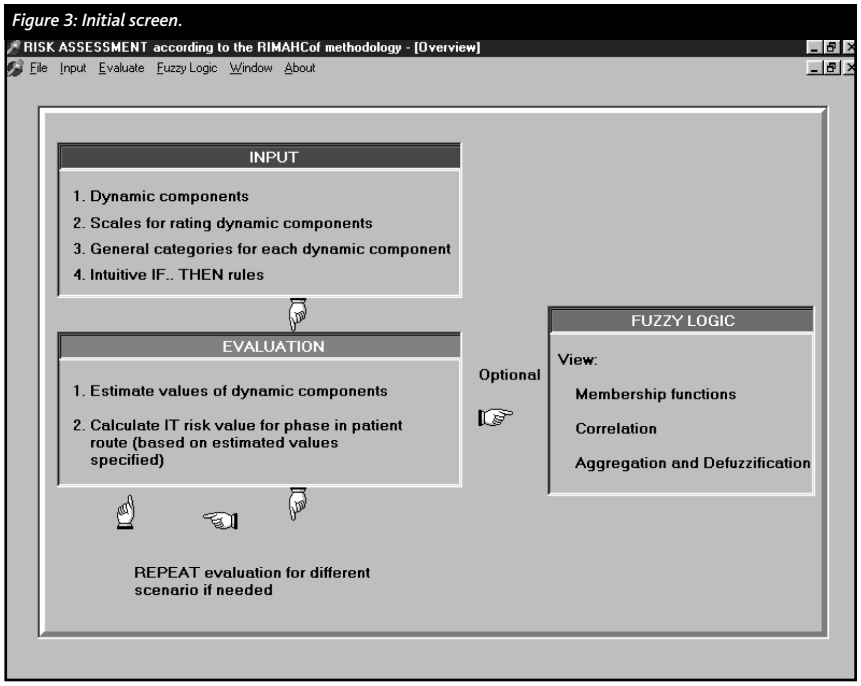
The prototype is aimed at enhancing risk assessment in health care by making use of a cognitive fuzzy-logic approach to assess the IT risks in this environment.

An overview of the various sections of the prototype

When the prototype is loaded, it presents the user with a GUI, as depicted in Figure 3.

This initial screen of the prototype presents an overview of the successive steps involved in using the prototype effectively to calculate an IT risk value for a specific phase in a patient route. According to this screen, the prototype can be viewed as consisting of three sections, namely the 'input' section, the 'evaluation' section and an optional 'fuzzy-logic' section. The 'input' section enables the user to enter all information required for calculating an IT risk value for a specific phase. This section needs to be completed first, before the 'evaluation' section can be executed. The 'evaluation' section involves the calculation of an IT risk value for a specific phase in a patient route, based on values entered with respect to the incidence of the dynamic components in this phase (for example, a typical patient spent more or less 30 minutes in a specific phase). This section can be executed repeatedly for as many scenarios as required. The third section of the prototype is optional and is principally aimed at an inspection of the cognitive fuzzy-logic approach followed to calculate the IT risk value of the specific phase.

Figure 3: Initial screen.



Functioning of the prototype

Following, a discussion on a real-life case in a bid more clearly to illustrate the functioning of the prototype.

Consider the 'recovery-ward' phase in the patient route depicted in Figure 2 (i.e., the route a typical patient would follow when admitted to hospital for an operation). Supposing we want to calculate the IT risk value for this phase by making use of the prototype and supposing that the dynamic components identified for this phase are the time spent in this phase, the number of communicating parties sharing patient information, the likelihood that risks will be exploited in this phase and the countermeasures access-control matrix and symmetric encryption, and that the technologies used to store and process patient information be paper files, database files, microfilm and a local-area network (LAN) (as depicted in Table 1).

Before implementing the prototype, one needs to distinguish between the inputs, i.e., the dynamic components that in some way contribute to the incidence of IT risks in that phase, and the output, i.e., the outcome of the interaction of the various input components in the specific phase. For the purposes of our case, the time spent in the 'recovery-ward' phase, the number of communicating parties sharing patient information in this phase and the countermeasures implemented and the technologies used to store and process the patient information (i.e., paper files, database files, microfilm and a LAN) are identified as the inputs to the prototype; the reason being that all these components in some way contribute to the likelihood that patient information will be exploited in the 'recovery-ward' phase. The likelihood that risks will be exploited in this phase is, therefore, identified as the output.

The 'input' section of the prototype

The 'input' section of the prototype requires that the user enter all information with respect to the *input* dynamic components needed to calculate an IT risk value for the specific phase. Information with respect to the output (i.e., the likelihood that risks might be exploited in this phase) is processed automatically by the prototype. The first input screen that needs to be populated is illustrated in Figure 4.

The prototype provides for eight possible input dynamic components. According to our case, we need to select all the dynamic components listed on this screen, except for the mainframe component.

In order to quantify the values of the incidence of the dynamic components in the 'recovery-ward' phase (for example, more or less three days are spent in this phase), appropriate scales of measurement need to be selected for each dynamic component identified. Such scale should include all allowable values for the component under consideration. A scale ranging from 0 to 30 days, for example, sufficiently represents the time a typical patient might spend in the 'recovery-ward' phase of the route he/she would follow when admitted to hospital for an operation. Figure 5 illustrates the input screen by means of which to select the scales for rating the dynamic components identified for this phase.

Figure 4: First input screen: dynamic components.

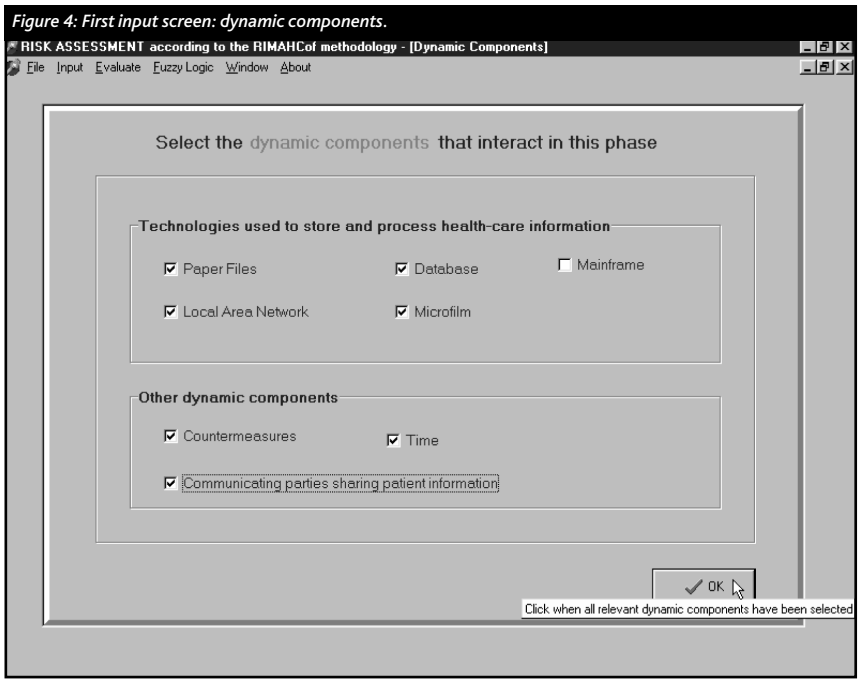


Figure 5: Second input screen: scales for rating dynamic components.

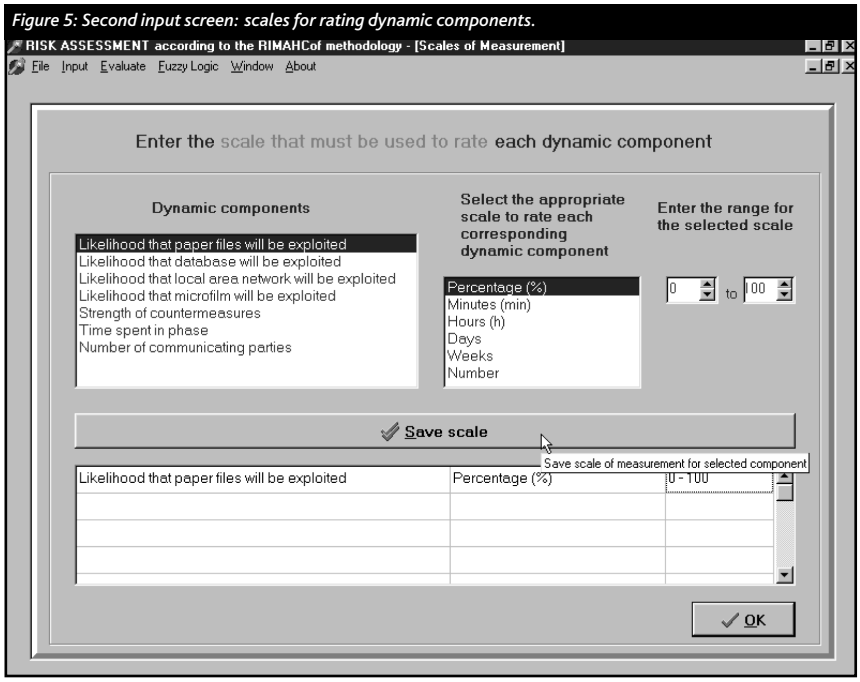
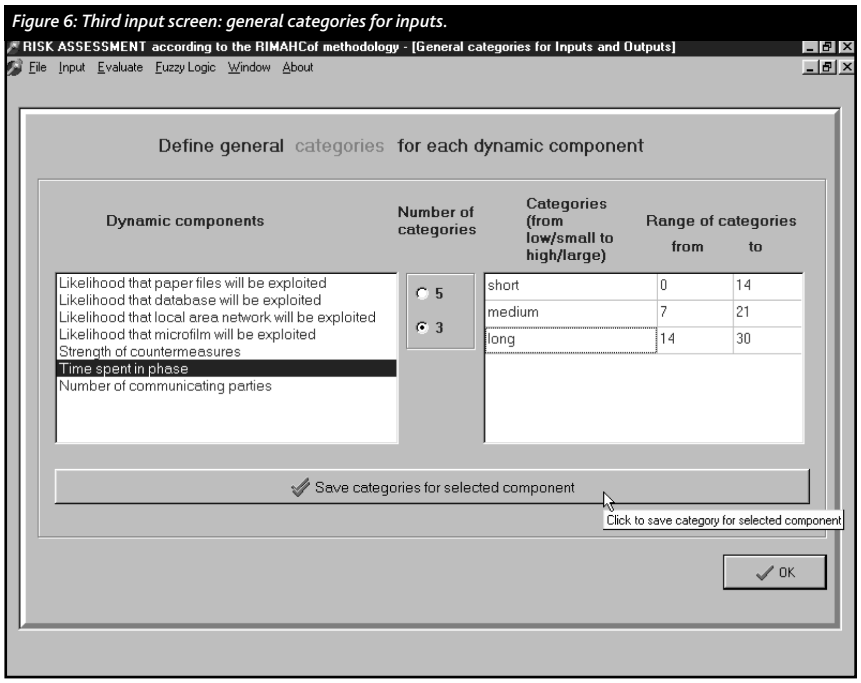


Figure 6: Third input screen: general categories for inputs.



All dynamic components pertaining to the 'recovery-ward' phase (as selected on the first input screen), as well as six possible scales for rating these components, are displayed on this input screen. Apart from selecting an appropriate scale for each dynamic component, the user also needs to define a range for the scale selected.

For the purposes of our case, we will select a scale ranging from 0 to 100% with which to rate the likelihood that paper files might be exploited (as depicted in Figure 5). The same scale is also selected for rating the strength of the countermeasures, the likelihood that database files might be exploited, the likelihood that the LAN might be exploited and the likelihood that the microfilm might be exploited. Furthermore, the time spent in the 'recovery-ward' phase is rated using a scale ranging from 0 to 30 days and, finally, we select a scale ranging from 0 to 100 to rate the number of communicating parties sharing patient information during this phase.

The incidence of a dynamic component merely constitutes a vague rather than an exact value. Such vague values define general categories, as opposed to rigid, fixed collections. A typical patient, for example, might spend a SHORT time in the 'recovery-ward' phase. These categories set more flexible membership requirements, thus allowing for partial membership to a category. The degree to which an input value of a component belongs under a category can be any value between 0 and 1 (rather than strictly 0 or 1). Eleven communicating parties sharing patient information in the 'recovery-ward' phase can, for instance, have a membership value of 0.8 in the 'SMALL number of communicating parties' category. In the realm of fuzzy logic, such categories are referred to as *fuzzy sets*.

Figure 7: Categories (fuzzy sets) for the inputs.

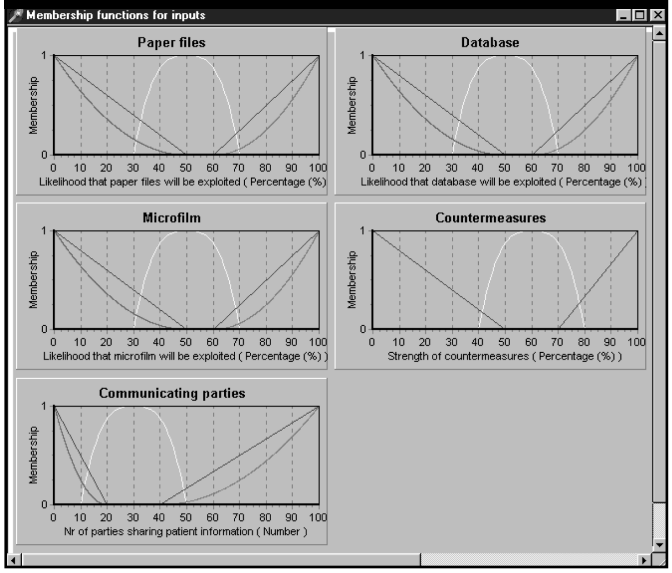
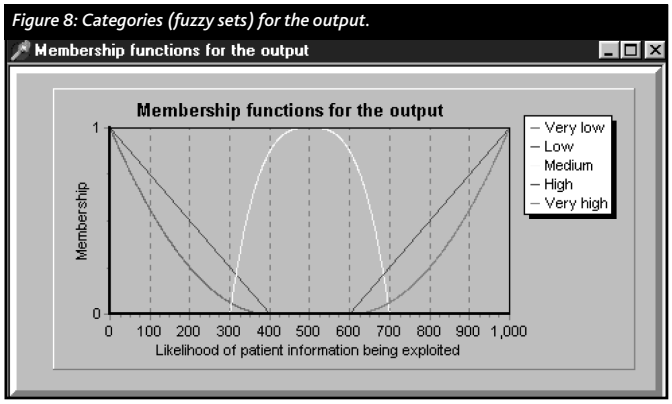


Figure 8: Categories (fuzzy sets) for the output.



In order to quantify the vague values of the input, such categories or fuzzy sets need to be identified for each input dynamic component of the 'recovery-ward' phase. These categories must, naturally, fall within the range of the rating scales defined for each dynamic component earlier. The categories defined for the inputs of this phase are listed in Appendix A of this paper.

Figure 6 represents the input screen, which needs to be populated with respect to these categories or fuzzy sets.

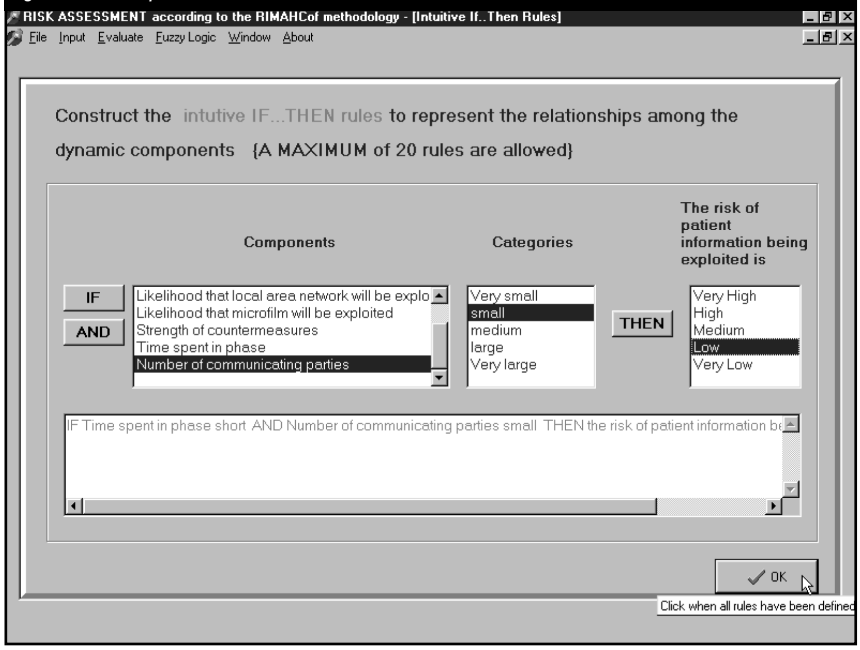
A category or fuzzy set represents a corresponding membership function that reflects the degree of membership in that category or fuzzy set by means of a given input value [43]. Figure 7 depicts the screen that is automatically generated by the prototype based on the categories or fuzzy sets, as defined in Appendix A. The drawing of such membership functions is a matter of common sense and engineering judgement.

The categories or fuzzy sets and membership functions for the output (i.e., the risk of patient information being exploited) are generated automatically by the prototype. These membership functions are graphically represented in Figure 8.

The viewing of both the input and the output membership functions forms part, however, of the 'fuzzy-logic' section of the prototype and is, therefore, optional.

The cognitive fuzzy-logic approach followed by the prototype to assess IT risks in a specific phase is based on intuitive linguistic IF…THEN rules. These rules (fuzzy rules) describe the relationships between the input components and the output. It is possible, for instance, intuitively to reason that, if the time spent in the 'recovery-ward' phase were SHORT and the number of communicating parties sharing patient information were SMALL, then the risk of patient information being exploited in this phase would be LOW. Human observation and intuition (which are subjective and vague by their very definition) form the basis of such intuitive or fuzzy rules. Figure 9 depicts the final input screen, which enables the user to construct intuitive IF…THEN rules such as these.

Figure 9: Fourth input screen: intuitive IF... THEN rules.



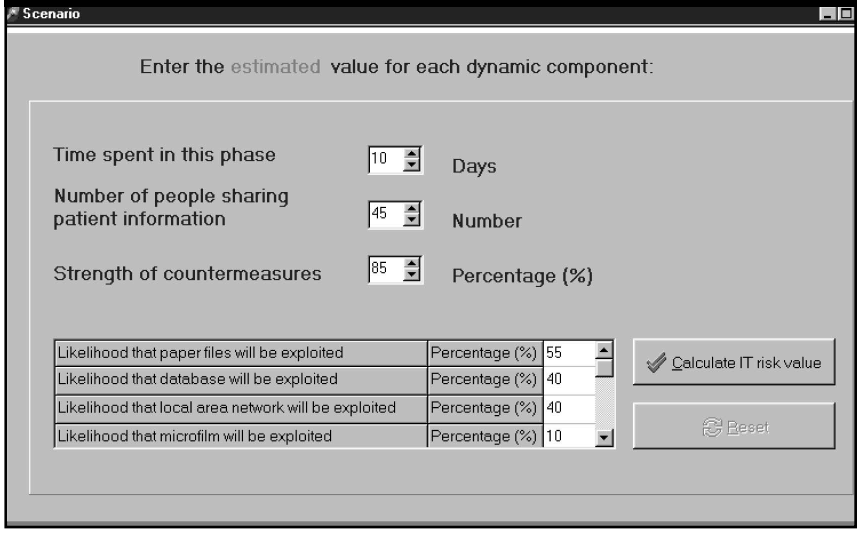
The rules formulated for our case are listed in Appendix B. Having populated this input screen, the 'evaluation' section of this prototype can commence.

The 'evaluation' section of the prototype

The 'evaluation' section of the prototype is aimed at calculating the IT risk value for a specific phase, using all the information entered by the user during the 'input' stage, as well as the values for the input components as observed by the user. Figure 10 depicts the screen used to enter these values, which values more or less describe the current scenario in the 'recovery-ward' phase.

Supposing that, after having observed the 'recovery-ward' phase, we conclude that a typical patient spends more or less 10 days in this phase. This constitutes memberships in

Figure 10: The current scenario in the 'recovery ward' phase.



both the 'SHORT time spent' and the 'MEDIUM time spent' categories or fuzzy sets. Furthermore, we conclude that approximately 45 communicating parties share patient information during this time. This constitutes memberships in the 'MEDIUM', 'LARGE' and 'VERY LARGE number of communicating parties' categories or fuzzy sets. The strength of the countermeasures already in place for this phase is rated at approximately 85% and, therefore, constitutes a membership in the 'STRONG strength of countermeasures' category or fuzzy set. As far as the technologies used to process and store patient information are concerned, we deem the likelihood that paper files might be exploited to be approximately 55%, the likelihood that the database might be exploited to be approximately 40%, the likelihood that the LAN might be exploited also to be approximately 40% and the likelihood that the microfilm might be exploited to be approximately 10% (as depicted in Figure 10). These values constitute memberships in the 'MEDIUM likelihood that paper files might be exploited' category or fuzzy set, memberships in the 'VERY LOW', 'LOW' and 'MEDIUM likelihood that the database might be exploited' categories or fuzzy sets and the 'likelihood that the LAN might be exploited' category or fuzzy set and memberships in both the 'VERY LOW' and 'LOW likelihood that the microfilm might be exploited' categories or fuzzy sets respectively.

Having entered all these values (as depicted in Figure 10), the IT risk value for the 'recovery-ward' phase can be calculated.

The 'fuzzy logic' section of the prototype

As was mentioned earlier, the prototype follows a cognitive fuzzy-logic approach to the assessment of IT risks. According to this approach, all the intuitive rules (as defined in Appendix B) fire in parallel to some degree. Some of the rules, however, fire to zero degrees, with the result that they will not contribute to the IT risk value of the 'recovery-ward' phase. According to our scenario (as depicted in Figure 10), seven of the intuitive rules (i.e., rule nos. 9, 10, 12, 15, 16, 17 and 18 listed in Appendix B) fire to a non-zero degree.

The next step in this approach would involve the mapping of the input categories or fuzzy sets implied by these intuitive rules (that fire to a non-zero degree) to the output categories or fuzzy sets. This process is called *correlation*. The correlation process for the first rule that fires to a non-zero degree is illustrated in Figure 11.

Figure 11: Correlation process.

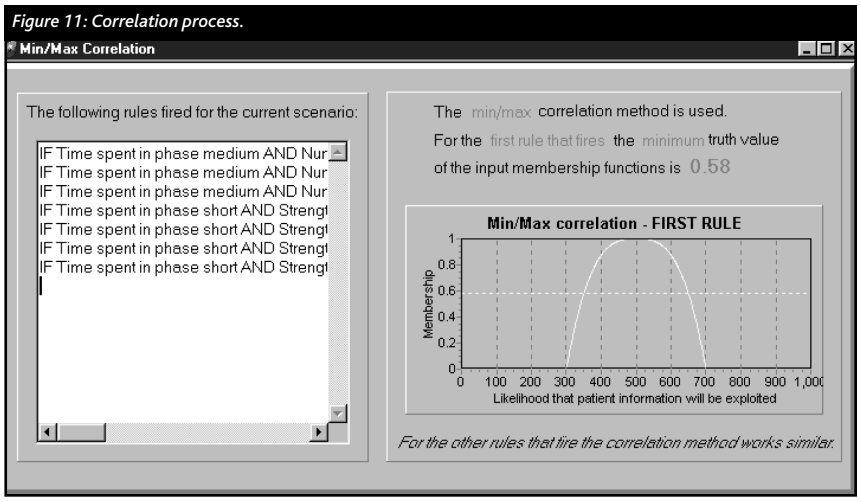


Figure 12: Aggregation and defuzzification process.

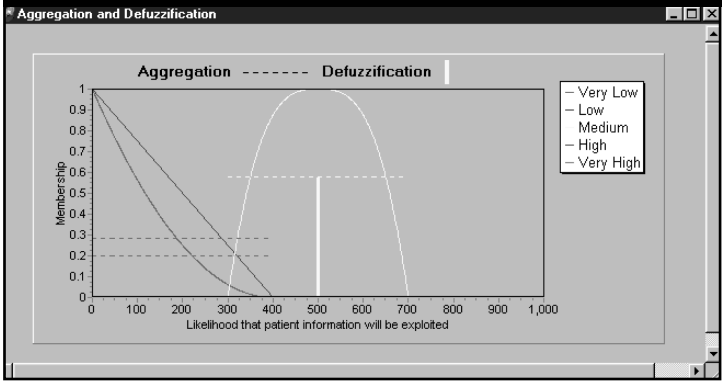
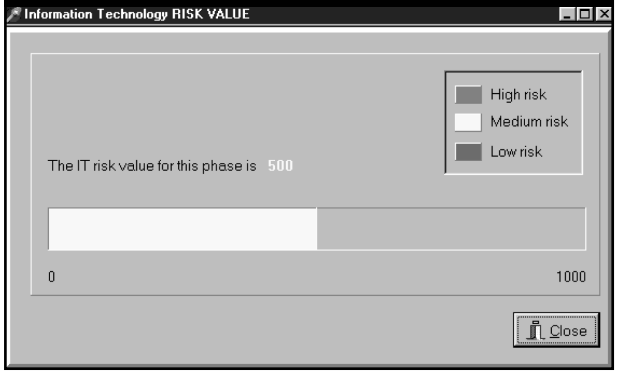


Figure 13: IT risk value for the 'recovery-ward' phase.



The next step in the cognitive fuzzy-logic approach would involve the *aggregation* of all output fuzzy regions generated thanks to the correlation process. This will result in a combined-output fuzzy region.

Finally, the last step in the cognitive fuzzy-logic approach would involve the *defuzzification* of the output region in a bid to obtain the expected IT risk value for the 'recovery-ward' phase. Both the aggregation and defuzzification processes are illustrated in Figure 12.

According to Figure 12, the 'recovery-ward' phase in the patient route under consideration has an IT risk value of 500 (as indicated by the solid vertical line). This phase is, therefore, classified as a medium-risk phase, as shown in Figure 13.

The fuzzy concepts, namely *correlation*, *aggregation* and *defuzzification*, are discussed in Appendix C of this paper.

Conclusion

This paper was devoted to expounding a prototype for assessing IT risks in the healthcare environment. The aim of the prototype, in turn, was to enhance the risk-assessment process specifically for the healthcare domain by following a cognitive fuzzy-logic approach to the assessment of its latent IT risks.

Appendix A

Categories defined for the inputs of the 'recovery-ward' phase in the route a typical patient would follow upon admission to hospital for an operation:

Dynamic component	Fuzzy set	Range
Likelihood that paper files will be exploited	Very low	0-50
	Low	0-50
	Medium	30-70
	High	60-100
	Very high	60-100
Likelihood that database will be exploited	Very low	0-50
	Low	0-50
	Medium	30-70
	High	60-100
	Very high	60-100
Likelihood that LAN will be exploited	Very low	0-50
	Low	0-50
	Medium	30-70
	High	60-100
	Very high	60-100
Likelihood that the microfilm will be exploited	Very low	0-50
	Low	0-50
	Medium	30-70
	High	60-100
	Very high	60-100
Strength of countermeasures	Weak	0-50
	Average	40-80
	Strong	70-100
Time spent in phase	Short	0-14
	Medium	7-21
	Long	14-30
Number of communicating parties	Very small	0-20
	Small	0-20
	Medium	10-50
	Large	40-100
	Very large	40-100

Appendix B

The IF...THEN rules (fuzzy rules) defined for representing the relationships between the inputs and the output:

IF the time spent in the 'recovery-ward' phase was LONG AND
the number of communicating parties sharing patient information was VERY LARGE AND
the likelihood of paper files being exploited was VERY HIGH AND
the strength of countermeasures was WEAK,
THEN the risk of patient information being exploited would be VERY HIGH.

IF the time spent in the 'recovery-ward' phase was LONG AND
the number of communicating parties sharing patient information was VERY LARGE AND
the likelihood of database files being exploited was VERY HIGH AND
the strength of countermeasures was WEAK,
THEN the risk of patient information being exploited would be VERY HIGH.

IF the time spent in the 'recovery-ward' phase was LONG AND
the number of communicating parties sharing patient information was VERY LARGE AND
the likelihood of the microfilm being exploited was VERY HIGH AND
the strength of countermeasures was WEAK,
THEN the risk of patient information being exploited would be VERY HIGH.

IF the time spent in the 'recovery-ward' phase was LONG AND
the number of communicating parties sharing patient information was VERY LARGE AND
the likelihood of the LAN being exploited was VERY HIGH AND
the strength of countermeasures was WEAK,
THEN the risk of patient information being exploited would be VERY HIGH.

IF the time spent in the 'recovery-ward' phase was LONG AND
the number of communicating parties sharing patient information was LARGE AND
the likelihood of paper files being exploited was HIGH AND
the strength of countermeasures was WEAK,
THEN the risk of patient information being exploited would be HIGH.

IF the time spent in the 'recovery-ward' phase was LONG AND
the number of communicating parties sharing patient information was LARGE AND
the likelihood of database files being exploited was HIGH AND
the strength of countermeasures was WEAK,
THEN the risk of patient information being exploited would be HIGH.

IF the time spent in the 'recovery-ward' phase was LONG AND
the number of communicating parties sharing patient information was LARGE AND
the likelihood of the microfilm being exploited was HIGH AND
the strength of countermeasures was WEAK,
THEN the risk of patient information being exploited would be HIGH.

IF the time spent in the 'recovery-ward' phase was LONG AND
the number of communicating parties sharing patient information was LARGE AND
the likelihood of the LAN being exploited was HIGH AND
the strength of countermeasures was WEAK,
THEN the risk of patient information being exploited would be HIGH.

IF the time spent in the 'recovery-ward' phase was MEDIUM AND
the number of communicating parties sharing patient information was MEDIUM AND
the likelihood of paper files being exploited was MEDIUM,
THEN the risk of patient information being exploited would be MEDIUM.

IF the time spent in the 'recovery-ward' phase was MEDIUM AND
the number of communicating parties sharing patient information was MEDIUM AND
the likelihood of database files being exploited was MEDIUM,
THEN the risk of patient information being exploited would be MEDIUM.

Appendix B continued...

IF the time spent in the 'recovery-ward' phase was MEDIUM AND
the number of communicating parties sharing patient information was MEDIUM AND
the likelihood of the microfilm being exploited was MEDIUM,
THEN the risk of patient information being exploited would be MEDIUM.

IF the time spent in the 'recovery-ward' phase was MEDIUM AND
the number of communicating parties sharing patient information was MEDIUM AND
the likelihood of the LAN being exploited was MEDIUM,
THEN the risk of patient information being exploited would be MEDIUM.

IF the time spent in the 'recovery-ward' phase was SHORT AND
the number of communicating parties sharing patient information was SMALL,
THEN the risk of patient information being exploited would be LOW.

IF the time spent in the 'recovery-ward' phase was SHORT AND
the strength of the countermeasures was STRONG,
THEN the risk of patient information being exploited would be LOW.

IF the time spent in the 'recovery-ward' phase was SHORT AND
the strength of the countermeasures was STRONG AND
the likelihood of paper files being exploited was VERY LOW,
THEN the risk of patient information being exploited would be VERY LOW.

IF the time spent in the 'recovery-ward' phase was SHORT AND
the strength of the countermeasures was STRONG AND
the likelihood of database files being exploited was VERY LOW,
THEN the risk of patient information being exploited would be VERY LOW.

IF the time spent in the 'recovery-ward' phase was SHORT AND
the strength of the countermeasures was STRONG AND
the likelihood of microfilm being exploited was VERY LOW,
THEN the risk of patient information being exploited would be VERY LOW.

IF the time spent in the 'recovery-ward' phase was SHORT AND
the strength of the countermeasures was STRONG AND
the likelihood of the LAN being exploited was VERY LOW,
THEN the risk of patient information being exploited would be VERY LOW.

The prototype has a number of important advantages. Firstly, it is user friendly, with the result that management would be able quite effectively to implement it without commanding thorough knowledge with respect to the actual cognitive fuzzy-logic approach followed by the prototype to assess IT risks. The prototype does, however, provide for an optional visual representation of the approach it follows, if and when required. The prototype is menu-driven and the steps that need to be followed when using the prototype are graphically illustrated on the opening screen. Another advantage of the prototype is that it enables the user to evaluate more than one scenario in a specific phase of a patient route without having to re-enter any information.

The prototype is specifically tailored to assess IT risks in the healthcare domain. Owing to their non-monetary nature, it would be extremely difficult, if not impossible, to quantify all the consequences of the possible risks to be incurred in this domain. This prototype, however, is novel in the sense that it takes into account the intuitive nature of human observation when assessing the latent IT risks in a healthcare institution. In addition, the prototype takes into account the vagueness of patient information (some part of the patient information could, for example, be of a confidential nature, whereas another part thereof, such as the geographical information, could well be unclassified).

Appendix C

There follow definitions of the fuzzy concepts applied by the prototype:

Correlation

The correlation process maps the input categories or fuzzy sets implied by the intuitive IF…THEN rules (fuzzy rules) that fire to a non-zero degree to the output categories (fuzzy sets). The prototype makes use of the correlation minimum method. This method truncates the relevant output category at the minimum-truth value of the relevant input categories [43-44].

Aggregation

In order to obtain a combined-output fuzzy region, all the output fuzzy regions generated as a result of the correlation process are aggregated. The aggregation method used by the prototype, namely the min/max aggregation, uses the maximum of the output fuzzy regions generated at each point along their mutual membership values to produce a final fuzzy region [43-44].

Defuzzification

In order to obtain the expected IT risk value for the 'recovery-ward' phase, the output region had to be defuzzified. Although there were several techniques available by means of which to effect defuzzification, the centre of maximum technique was used to determine the expected IT risk value for the 'recovery-ward' phase in the present prototype. The 'centre of maximum defuzzification' technique was used to locate the domain point in the aggregated output region with the maximum truth [43-44].

The RiMaHCoF methodology specifically focuses on the *confidentiality* of patient information. The other four Information Security services (identification and authentication, authorization, integrity and non-repudiation) do not form part of the Information Security scope of the proposed model. Further research should, therefore, be conducted into the remaining Information Security services.

Another area that will bear further research is the way in which the proposed IT risk-management model could be adapted to suit organizations in other business sectors and industries. The patient information route, which plays a pivotal role in the proposed model, might, for instance, be replaced by a transaction route in business enterprises. In this way, organizations in other sectors or industries may also benefit from the proposed IT risk management model.

References

[1] *Blobel, B. 1997. Security requirements and solutions in distributed electronic health records. In: Proceedings of the 13th IFIP TC 11 International Conference on Information Security. Great Britain: Chapman & Hall, 1997, pp. 377-389.*

[2] *Bakker, A.R., Barber, B., Tervo-Pellikka, R. and Treacher, A. (Eds.), 1995. Communicating health information in an insecure world. In: Proceedings of the Helsinki Working Conference. Amsterdam: Elsevier Science, 43: 1, 2.*

[3] *Grissonnanche, A., 1986. Security and protection in information systems. In: Proceedings of the fourth IFIP TC 11 International Conference on Computer Security, IFIP/Sec '86. Monte Carlo: Monaco.*

[4] *Barber, B., Garwood, D. and Skerman, P., 1994. Security in hospital information systems. In: Security and data-protection program presented at the IMIA WH10 Working Conference in Durham.*

[5] *Furnell, S.M. and Sanders, P.W., 1995. Security management in the healthcare environment. In: Greenes, R.A., Peterson, H.E. and Protti, D.J. (eds.). MEDINFO '95. Proceedings of the eighth World Congress on Medical Informatics. Vancouver Trade & Convention Centre: Canada. pp. 675-678.*

[6] *Barber, B., Treacher, A. and Louwerse, K., 1996. Data security for healthcare. Amsterdam: IOS Press. p. 246. Studies in Health Technology Informatics, Vol. 31-33.*

[7] *Rossing, N. SEISMED: a secure environment for information systems in medicine. Presentation note of the program AIM of DGXIII.*

[8] Patel, A. and Kantzavelou, I., 1995. Implementing network-security guidelines in healthcare information systems. In: Greenes, R.A., Peterson, H.E. and Protti, D.J. (eds.). MEDINFO '95. Proceedings of the eighth World Congress on Medical Informatics. Vancouver Trade & Convention Centre, Canada, pp. 671-674.

[9] Ziegler, B., 1980. Data protection in medical research. In: Lindberg, D.A.B. and Kaihara, S. (eds.). MEDINFO '80. Proceedings of the third World Congress on Medical Informatics. IFIP: North-Holland, pp. 316-318.

[10] Ginneken, A.M., 1994. Computer-based patient records. In: Van Bemmel, J.H. and McCray, A.T. (eds.). Yearbook '94 of Medical Informatics. Advanced communications in health care. Schattauer, pp. 173-175.

[11] Kenny, D.J., 1983. Discussions and conclusions. In: Griesser, G., Jardel, J.P. and Sauter, K. Data protection in health information systems. Where do we stand? Proceedings of the IFIP IMIA WG 4 Working Conference on Data Protection in Health Information Systems. 1983. North-Holland: Elsevier Science, pp. 219-235.

[12] Heinlein, E.B., 1996. Medical records security. Computers & Security, Vol. 15, No. 2, pp. 100-102.

[13] Lincoln, T.L. and Essin, D., 1991. The computer-based patient record: issues of organisation, security and confidentiality. In: Database Security, 5: Status and Prospects. Results of the IFIP G 11.3 Workshop. 1992. Amsterdam: North-Holland, pp. 1-19.

[14] Kohn, P., 1995. Computer-based patient record systems: the future of health care is in digital technology. INFORM, 38-46, Nov/Dec.

[15] Brannigan, V.M. and Beier, B.R., 1995. Patient privacy in the era of medical computer networks: a new paradigm for a new technology. In: Greenes, R.A., Peterson, H.E. and Protti, D.J. (eds.). MEDINFO '95. Proceedings of the eighth World Congress on Medical Informatics. Vancouver Trade & Convention Centre, Canada, pp. 640-643.

[16] Calcote, S., 1997. Developing a secure healthcare information network on the Internet. Healthcare Financial Management, January, 1997, p. 68.

[17] Gritzalis, D., Katsikas, S., Keklikoglou, J. and Tomaras, A., 1992. Determining access rights for medical information systems. Computers & Security, Vol. 11, No. 2, pp. 149-161.

[18] Iversen, K.R., Heimly, V. and Lundgren, T.I., 1995. Implementing security in computer-based patient records. Clinical Experiences. In: Greenes, R.A., Peterson, H.E. and Protti, D.J. (eds.). MEDINFO '95. Proceedings of the eighth World Congress on Medical Informatics. Vancouver Trade & Convention Centre, Canada, pp. 657-660.

[19] Holbein, R., Teufel, S., Morger, O. and Bauknecht, K., 1997. A comprehensive need-to-know access-control system and its application for medical information systems. In: Proceedings of the 13th IFIP TC 11 International Conference on Information Security. Great Britain: Chapman & Hall, pp. 33-414.

[20] Miller, M. and Cooper, J., 1996. Security considerations for present and future medical databases. International Journal of Bio-Medical Computing, Vol. 41, pp. 39-46.

[21] Pangalos, G.J., 1994. Medical Database Security Policies. In: Van Bemmel, J.H. and McCray, A.T. Yearbook '94 of Medical Informatics. Advanced communications in health care. Schattauer IMIA. pp. 253-259.

[22] Biskup, J., Morgenstern, M. and Landwehr, C.E., 1994. Database Security: Status and Prospects. In: results of the IFIP WG 11.3 Workshop on Database Security. Germany.

[23] Kaplan, J.G., 1992. Protecting sensitive medical information. In: Database Security, 6: Status and Prospects. IFIP WG 11.3 Workshop. Amsterdam: North-Holland. 1993. pp. 1-14.

[24] Pangalos, G. and Khair, M., 1996. Design of secure medical database systems. SACJ/SART, 17, pp. 45-53.

[25] Pangalos, G., Gritzalis, D., Khair, M. and Bozios, L., 1995. Improving the security of medical database systems. In: Eloff, J.H.P. and Von Solms, S.H. (eds.). Information security – the next decade: Proceedings of the 11th IFIP TC 11 International Conference on Information Security. Great Britain: Chapman & Hall, pp. 11-25.

[26] Gritzalis, D., Katsikas, S., Keklikoglou, J. and Tomaras, A. 1991. Data security in medical information systems: the Greek case. Computers & Security, Vol. 10, No. 2, pp. 141-159.

[27] Gritzalis, D., Katsikas, S., Keklikoglou, J. and Tomaras, A., 1992. Determining access rights for medical information systems. Computers & Security, Vol. 11, No. 2, pp. 149-161.

[28] Gritzalis, D., Katsikas, S., Keklikoglou, J. and Tomaras, A., 1991. Data security in medical information systems: the Greek case. Computers & Security, Vol. 10, Nio. 2, pp. 141-159.

[29] Pangalos, G.J., 1996. Secure medical databases: design and operation. International Journal of Bio-Medical Computing, 43: 53-60.

[30] Davey, J. The role of risk analysis in European harmonisation of security for healthcare information systems. Computer Methods and Programs in Biomedicine, 48(1, 2): 133-137.

[31] Gritzalis, D., Kantzavelou, I., Katsikas, S. and Patel, A., 1995. A classification of health information systems security flaws. In: Eloff, J.H.P. and Von Solms, S.H., (eds.). Information security – the next decade: Proceedings of the 11th IFIP TC 11 International Conference on Information Security. Great Britain: Chapman & Hall, pp. 454-464.

[32] Barber, B. and Davey, J., 1992. The use of the CCTA risk analysis and management methodology [CRAMM] in health information systems. In: Degoulet, P., Lun, K.C., Piemme, T.E. and Rienhoff, O. (eds.). MEDINFO '92. North-Holland: Elsevier Science, pp. 1589-1593.

[33] Warren, M.J., Furnell, S.M. and Sanders, P.W., 1997. ODESSA: a new approach to healthcare risk analysis. In: Proceedings of the 13th IFIP TC 11 International Conference on Information Security. Great Britain: Chapman & Hall, pp. 391-401.

[34] Robinson, D.M., 1992. A legal examination of format, signature and confidentiality aspects of computerised health information. In: Lun, K.C. (eds.). MEDINFO '92. North-Holland: Elsevier Science, pp. 1554-1560.

[35] Eloff, J.H.P. and Smith, E., 1999. Security in healthcare information systems – current trends. International Journal of Medical Informatics, 54: 39-54.

[36] Labuschagne, L., 1992. "Inligtingsekerheid, met spesifieke verwysing na risiko-ontleding." Rand Afrikaans University. Johannesburg, South Africa (dissertation (MCom) – RAU).

[37] Security in computing. Charles P. Pfleeger. Second edition. Prentice-Hall International Inc., USA, 1997, p. 574.

[38] Badenhorst, K.P. and Eloff, J.H.P., 1989. Framework of a methodology for the life-cycle of computer security in an organization. Computers & Security, Vol. 8, pp. 433-442.

[39] Barber, B. and Davey, J., 1992. The use of the CCTA risk analysis and management methodology [CRAMM] in health information systems. In: Degoulet, P., Lun, K.C., Piemme, T.E. and Rienhoff, O. (eds.). MEDINFO '92. North-Holland: Elsevier Science, pp. 1589-1593.

[40]Warren, M.J., Furnell, S.M. and Sanders, P.W., 1997. ODESSA: a new approach to healthcare risk analysis. In: Proceedings of the 13th IFIP TC 11 International Conference on Information Security. Great Britain: Chapman & Hall, pp. 391-401.

[41]Eloff, J.H.P. and Smith, E., 1998. Modelling risks in a healthcare institution. In: Proceedings of the 14th IFIP TC 11 International Conference on Information Security. Austria: Austrian Computer Society, pp. 592-598.

[42]Eloff, J.H.P. and Smith, E., 1999. Cognitive fuzzy modelling for enhanced risk assessment in a healthcare institution. IEEE Intelligent Systems and their Applications,15(2): 69-75.

[43]Kosko, B., 1997. Fuzzy engineering. New Jersey: Prentice-Hall, p. 549.

[44]Cox, E.D., 1994. The fuzzy systems handbook: a practitioner's guide to building, using and maintaining fuzzy systems. Boston: Academic Press, p. 515.

[45]Pearl, J. 1984. Heuristics. Intelligent search strategies for computer problem-solving. Canada: Addison-Wesley, p. 382.