Artificial Intelligence Applications for Risk Analysis, Risk Prediction and Decision Making in Disaster Recovery Planning

Masoud Mohammadian

University of Canberra
Faculty of Information Sciences and Engineering
Canberra, ACT 2606, Australia
Masoud.Mohammadian@canberra.edu.au

Abstract. Development and management of disaster recovery plan for IT systems are complex, demanding, and yet crucial to an organization success and its competitive position in the marketplace. Due to rapid changes in emerging technologies there is a need for constant improvement and adjustment to disaster recovery plans for IT systems. There are a large number of processes involved in disaster recovery planning for IT system. The interdependencies of these processes make it very difficult for Chief Information Officers (CIOs) to comprehend and be aware of effect of inefficiencies that may exist in development of these processes in the disaster recovery plan of their organization. This paper considers the implementation of a Fuzzy Cognitive Maps (FCM) to provide facilities to capture and represent complex relationships in implementing a disaster recovery plan for IT systems and their related processes to improve the understanding of CIOs about the systems and its associated risks.

Keywords: Fuzzy Cognitive Maps, Disaster Recovery Planning, Risk Analysis, Monitoring, Scenario Analysis, Decision Making

1 Introduction

The consequence of natural or man-made disasters to organizations can cause organizations to suffer financially, and damage the image of organisations as well as damaging its relationships with its customers, its business partners, and the public. From 250 organizations that were surveyed by [1] to determine trends and problems in disaster recovery planning and preparation, it was found that three of every ten organizations surveyed in [1] have been through a disaster. From the same survey conducted it was found that nearly three of every four organizations reported having a disaster recovery plan in place. However, disaster recovery planning is still a new process in many organizations.

Disaster recovery planning is the process of assessing risks that may cause damage to an organization then developing, documenting, implementing, testing, and maintaining procedures that assists the organization to return to normal operations with minimum losses after a disaster [1, 2, 3].

Constructing a disaster recovery plan for an organisation can be a very tedious, complicated and laborious task depending on the size and type of the organisation. A disaster recovery plan must meet all needs of the organization for which the disaster recovery plan is constructed. It should recognize and take in consideration the organization's characteristics such as size and type of organization, resources, number of employees and customers, type and breath and depth of possible disasters and requirements for operation and processes [1, 2, 3, 4]. All policies and procedures in a disaster recovery plan must support the critical needs of business operations and it should comply with all organization and government relevant laws and regulations. Managers in three of every ten organizations surveyed by [1] think the worst disaster would involve outages of IT services and loss of customer data. Emerging technologies change rapidly and that needs to be reflected in the organization's disaster recovery plan. Therefore there is a need for constant improvement and adjustment to disaster recovery plans to reflect changes in IT systems of an organization. There are a large number of processes involved in disaster recovery planning for IT system. These processes have interdependencies and sometimes are difficult to comprehend. Therefore there is a need for continues monitoring, improvement and assessment of disaster recovery plans. Only by using simulation it is possible to find out exactly the possible hidden flaws in disaster recovery plans. Simulations of possible disasters are however expensive and interruptive to organisation's day to day functions and although it is required, it is not possible to be organised in regular basis.

In this paper Fuzzy Cognitive Maps (FCMs) [5, 6] are suggested as a method for monitoring and risk analysis for disaster recovery plans. FCMs can capture and represent complex relationships involved in implementing a disaster recovery plan and their related processes to improve the understanding of CIOs about their systems and its associated risks in their organizations. By using FCMs CIOs can regularly review and improve their disaster recovery plans. They can use simulation to access undesirable situations that may occur due to a disaster and evaluate the result of such situations. CIO's can provide greater improvement in development, monitoring and maintenance of disaster recovery plans for IT facilities and perform what-if analysis to better understand vulnerabilities in their organisation's disaster recovery plans.

Next section provides a brief overview of requirements of a disaster recovery plan. Fuzzy Cognitive Maps (FCMs) are then introduced in section 3. Simulations using FCM for risk analysis using what-if scenario are provided in section 4. Simulations results are provided in section 4. The paper then concludes in section 5.

2 Disaster Recovery Plan

A disaster recovery plan defines and documents the chain of command of the managers responsible for declaring, responding to, and recovering from a disaster. The plan specifies the role of each team in each department and outside support organization in a disaster. It facilitates control of communications among decision-makers, managers, and staff, and external support organizations, law enforcement, emergency services, media and other external entities.

All teams of employees involved in disaster recovery response must be trained to implement documented policies and procedures and to address problems correctly and according to the disaster recovery plan. Disaster recovery procedures are tested, rehearsed and monitored regularly to determine weaknesses in the disaster recovery plan procedures. The results of testing procedures of a disaster recovery plan are used for evaluations and to modify the plan, procedures, or training [1].

New threats and business conditions needs to be tested as they develop. The disaster recovery plans and procedures then are required to be tested and monitored with new changes accordingly [1, 2]. The results of these evaluations are then implemented as new policies and procedures in the organization's disaster recovery plan. Next sub-sections consider the principles of disaster recovery plan.

2.1 Process of Disaster Recovery Planning

The first essential principle of disaster recovery plan is the support and participation of upper-level management of all business units. According to [1] the process of disaster recovery planning can be broken down into eight major steps. Each step is interrelated and consists of processes and sub-processes and each step builds upon the others. These steps are namely, organizing the team, assessing risks in the enterprise, establishing roles across departments and organizations, developing policies and procedures, documenting disaster recovery procedures, preparing to handle disasters, training, testing, and rehearsal, ongoing management and monitoring. These are shown in Figure 1.

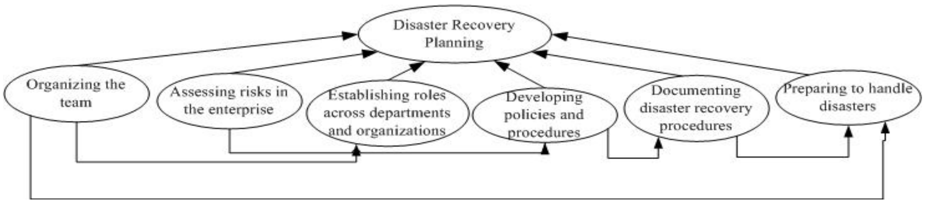

Disaster Recovery Planning
Organizing the team
Assessing risks in the enterprise
Establishing roles across departments and organizations
Developing policies and procedures
Documenting disaster recovery procedures
Preparing to handle disasters

Fig. 1. Disaster Recovery Planning steps [1]

Building a disaster recovery plan can take many months or in special cases many years [1, 2].

2.2 Organizing the Disaster Recovery Planning Team

First step in developing a disaster recovery plan is organizing the planning team to develop a disaster recovery plan. The team must represent all the functions of an organization. The teams should be trained in disaster recovery planting by attending professional training sessions [1]. This step includes, Training Disaster Recovery Team, Setting the Planning team schedules, Starting awareness campaign, Budgeting Disaster Recovery Planning and Management and finally coping Standards and Regulatory Bodies. Figure 2. Displays the processes involved in step 1 (i.e. Organizing the Disaster Recovery Planning Team)

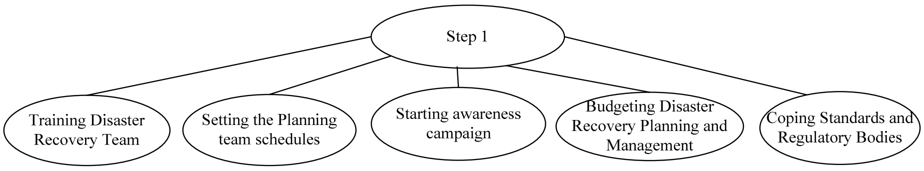

Step 1
Training Disaster Recovery Team
Setting the Planning team schedules
Starting awareness campaign
Budgeting Disaster Recovery Planning and Management
Coping Standards and Regulatory Bodies

Fig. 2. Displays the processes involved in step 1 (i.e. Organizing the Disaster Recovery Planning Team)

2.3 Assessing Risks in the Enterprise

Assessing the risk that an enterprise faces is the step 2 in developing a disaster recovery planning. It consists of business impact analysis to assess risks and determining the potential economic loss that could occur as a result of such risks.

Second step (i.e. Assessing Risks in the Enterprise) in developing a disaster recovery plan include: Collecting risk assessment data, Inventory documenting business processes, Create business processes inventory, Identify and categorize treats and vulnerabilities, Measuring and qualifying treats, and Compiling risk assessment reports. Figure 3. Displays the processes involved in step 2 of disaster recovery planning [1].

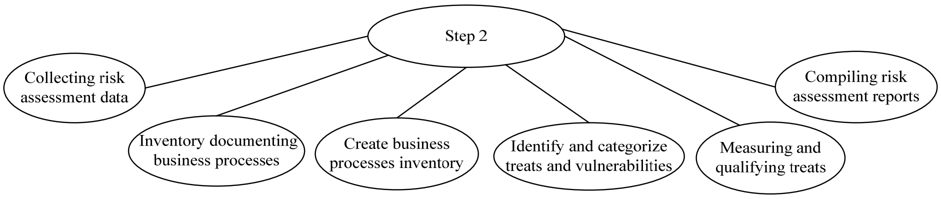
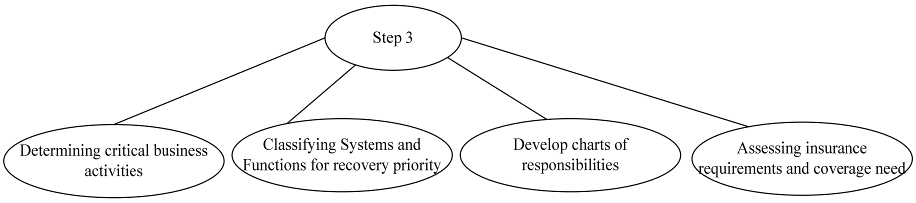

Step 2
Collecting risk assessment data
Inventory documenting business processes
Create business processes inventory
Identify and categorize treats and vulnerabilities
Measuring and qualifying treats
Compiling risk assessment reports

Fig. 3. Displays the processes involved in step 2 of disaster recovery planning

2.4 Establishing Roles Across Departments and Organization

This step consists is to establish the roles that each department, business partner, and outside service organization plays in disaster recovery. The third step (i.e. Establishing Roles Across Departments and Organization) in developing a disaster recovery plan include: Determining critical business activities, Classifying Systems and Functions for recovery priority, Develop charts of responsibilities, and Assessing insurance requirements and coverage needs [1].

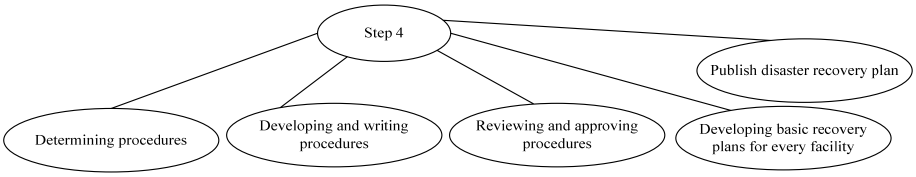

Step 3
Determining critical business activities
Classifying Systems and Functions for recovery priority
Develop charts of responsibilities
Assessing insurance requirements and coverage need

C1 = Determining critical business activities, C2 = Classifying Systems and Functions for recovery priority, C3 = Develop charts of responsibilities, C4 = Assessing insurance requirements and coverage needs

Fig. 4. Displays the processes involved in step 3 of disaster recovery planning

2.5 Developing Policies and Procedures

Disaster recovery procedures are step-by-step methods designed to restore an organizational function or business process [1]. All departments, organizations, in all locations, with all involved staff must assist in development of these procedures. The fourth step (i.e. Developing Policies and Procedures) in developing a disaster recovery plan include: Determining what disaster recovery procedures are needed to be developed, Developing and writing disaster recovery procedures, Reviewing and approving disaster recovery procedures, Developing basic recovery plans for every facility, and Publish disaster recovery plan.

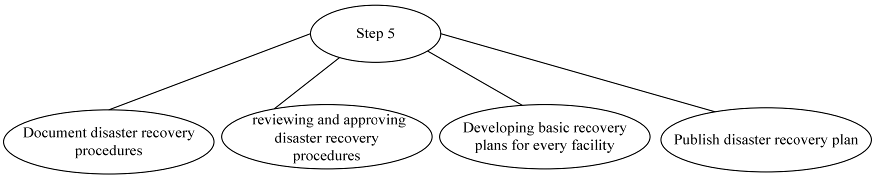

Step 4
Publish disaster recovery plan
Determining procedures
Developing and writing procedures
Reviewing and approving procedures
Developing basic recovery plans for every facility

C1 = Determining procedures, C2 = Developing and writing procedures, C3 = Reviewing and approving procedures, C4 = Developing basic recovery plans for every facility, and C5 = Publish disaster recovery plan

Fig. 5. Displays the processes involved in step 3 of disaster recovery planning

2.6 Documenting Disaster Recovery Procedures

This step in developing a disaster recovery plan is to document the policies and procedures developed in the previous step. Documentations need to be reviewed and updated on regular basis. This step (i.e. Documenting Disaster Recovery Procedures) in developing a disaster recovery plan include: Document disaster recovery procedures developed, reviewing and approving disaster recovery procedures, Developing basic recovery plans for every facility, Publish disaster recovery plan [1].

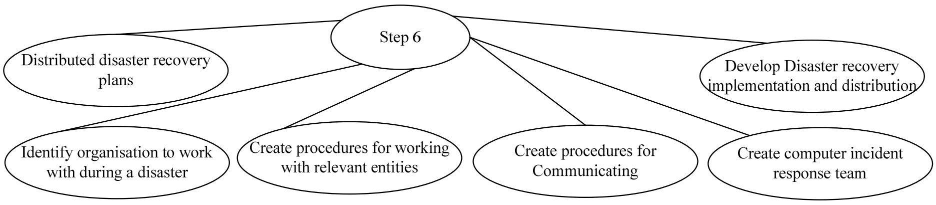

Step 5
Document disaster recovery procedures
reviewing and approving disaster recovery procedures
Developing basic recovery plans for every facility
Publish disaster recovery plan

C1 = Document disaster recovery procedures developed, C2 = reviewing and approving disaster recovery procedures, C3 = Developing basic recovery plans for every facility, C4 = Publish disaster recovery plan

Fig. 6. Documenting Disaster Recovery Procedures

2.7 Preparing to Handle Disasters

During this step the disaster recovery plan is distributed to all of departments, organizations, and employees involved in disaster response and recovery. This step (i.e. Preparing to handle disaster) in developing a disaster recovery plan include: Distributing disaster recovery plans to all of the departments, organizations, and employees involved in disaster response and recovery, Identifying organisation to work with during a disaster, Creating procedures for working with public service provider, insurance companies, private service providers, business arena, Creating procedures for Communicating with media and stakeholders, Creating procedures for Communicating with law enforcement agencies, Creating procedures for IT recovery, Creating computer incident response team, Developing Disaster recovery implementation team, Assigning responsibility, Establishing implementation schedule [1].


Step 6
Distributed disaster recovery plans
Develop Disaster recovery implementation and distribution
Identify organisation to work with during a disaster
Create procedures for working with relevant entities
Create procedures for Communicating
Create computer incident response team

C1 = Distributed disaster recovery plans to all of the departments, organizations, and employees involved in disaster response and recovery, C2 = Identify organisation to work with during a disaster, C3= Create procedures for working with public service provider, insurance companies, private service providers, business arena, create procedures for Communicating with media and stakeholders, and create procedures for IT recovery, C4 = Create computer incident response team, C5 = Develop Disaster recovery implementation team and assign responsibility and establish implementation schedule, and distribute Disaster Recovery documents

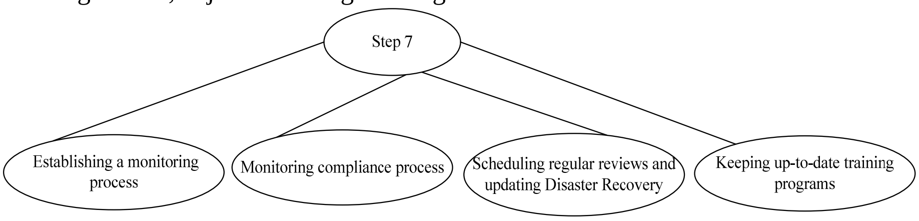
Fig. 7. Prepare to handle disasters

2.8 Training, Testing, and Rehearsal

This step of the disaster recovery plan is to test and rehearse parts of the disaster recovery plan. Finally a live simulation must be conducted. This steps includes: Test and rehearse disaster recovery plans and procedures, Use step by step testing procedures, Develop test scenarios (This task may be automated and case scenarios can be developed using AI techniques such Genetic and Evolutionary Algorithms), Rehearse the ability of subunits to execute disaster recovery procedures, Measure the effectiveness of disaster recovery plans and procedures and fine-tune team

2.9 Ongoing Management

The last step in disaster recovery planning is to assess the emergence of new and evolving threats, adjust for changes in organizational structure.


Step 7
Establishing a monitoring process
Monitoring compliance process
Scheduling regular reviews and updating Disaster Recovery
Keeping up-to-date training programs

C1 = Establishing a monitoring process, C2 = Monitoring compliance process, C3 = Scheduling regular reviews and updating Disaster Recovery documents, C4 = Keeping up-to-date training programs

Fig. 8. Ongoing Management

The impact of new IT infrastructures and network technologies on recovery procedures must also be determined. For multinational organisations changes in legal requirements, as well as political climate in the related countries must be considered, documented and implemented in a new version of the disaster recovery plan. This step consists of: Establishing a monitoring process, Monitoring compliance process, Scheduling regular reviews and updating Disaster Recovery documents, and Keeping up-to-date training programs [1].

A disaster recovery plan should reflect the organization’s need to include the reliance of the organization’s on computer systems and IT communications networks and infrastructures. IT manages must be involved in risk assessment and business impact analysis of IT and network infrastructures. With evolution of computer systems and networks in an organization disaster recovery plan and procedures must be evolved and updated on regular basis.

3 Fuzzy Cognitive Maps

Fuzzy Cognitive Maps (FCM) [5, 6] are graph structures that provide a method of capturing and representing complex relationships in a system. Application of FCM has been popular in modelling problems with low or no past data set or historical information [5, 6].

A FCM provides-the facilities to capture and represent complex relationships in a system to improve the understanding of system designers. A FCM uses scenario analysis by considering several alternative solutions to a given situation. Concepts sometimes called nodes or events represent the system behaviour in a FCM. The concepts are connected using a directed arrow showing causal relations between concepts. The graph's edges are the casual influences between the concepts. The development of the FCM is based on the utilization of domain experts' knowledge. Expert knowledge is used to identify concepts and the degree of influence between them.

Kosko [6] enhanced cognitive maps by including fuzzy values for the relationships between concepts. FCM allows capturing and representing complex relationships. A FCM describes a system as a directed graph. Concepts are connected using a directed arrow showing causal relations between concepts. The graph's edges are the casual influences between the concepts. The value of a node reflects the degree to which the concept is active in the system at a particular time. This value is a function of the sum of all coming (weights) edges multiplied and the value of the original concept at the immediately preceding state. A threshold function applied to the weighted sums. Values on each edge indicate relationships between concepts. These values indicate whether one concept increases or decreases the likelihood of another concept. The edges have values in the interval range [-1, 1]. These values indicate the degree to which one concept affects another. A positive relationship between two concept 1 (C1) and concept 2 (C2) indicates an increase in the likelihood of concept 2 to occur. Negative-values indicate a decrease in the likelihood of concept 2 occurring. The FCM can represent concepts of a disaster recovery plan model as described above. These relationships indicate whether one increases or decreases the likelihood of another event/process [5, 6]. The disaster recovery plan model as described above and shown in Figure 1 can be converted into a FCM (see Figure 9). Executives, managers, and staff involved in disaster recovery planning in an organization are the experts and they are required to provide leadership in this area and they can determine the weights of the different causal links and the initial activation level for each concept on FCM model used for disaster recovery plan analysis and monitoring. In this scenario the author has carefully considered the disaster recovery plan steps as described above including all processes involved and provided the weights for the FCM as shown in Figure 9. The weights and the activation function value vary for different organization based on the size, budget, priorities and importance of processes (concepts) for the given organization. This will give the freedom to an organization to evaluate each concept and provide weights and activation function values based on the organization's priorities, preferences, market understanding, budget constraints, strategic aims and other measures of their organization.

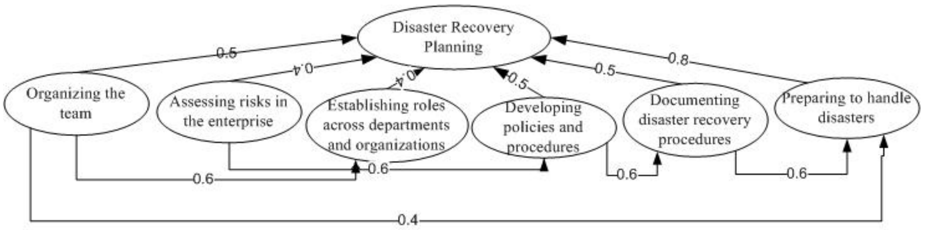

Disaster Recovery Planning
0.5
0.4
0.4
0.5
0.5
0.8
Organizing the team
Assessing risks in the enterprise
Establishing roles across departments and organizations
Developing policies and procedures
Documenting disaster recovery procedures
Preparing to handle disasters
0.6
0.6
0.6
0.6
0.4

Fig. 9. A FCM representation of concepts of the disaster recovery planning model with weights allocated to each edge

The mathematical model behind the graphical representation of the FCM consists of a lxn state vector l. This state vector represents the values of the n concepts and nxn weight matrix W_{ij} represents value of weights between concepts of C_i, and C_j. For each concept in a FCM a value one or zero is assigned. One represents the existence of that concept at a given time and zero represent none-exist of the respective concept. A threshold function is used in a FCM. The threshold function used in this research study is sigmoid function [5, 6]. The threshold value is set to be 0.5.

$$C_i\,(t_{n+1}) = S\left[\sum_{K=1}^{N} e_{KI}\,(t_n) C_k\,(t_n)\right] \qquad (1)$$

Now a FCM model can be used to identify and access risks that may arise due to unavailability or shortcomings of different concepts in the FCM model for disaster recovery planning analysis and assessment for a given organization. The FCM can be used to provide executives with possibilities for what-if analysis to understand the vulnerability in each layers of the FCM model and to perform risk analysis and risk identification in that model. Some of the possible what-if scenario analysis and questions that can be performed are:

What are the benefits of training and assigning the correct roles across departments to the disaster recovery plan of the organization?

What are the influences of correct policies in overall success of the disaster recovery plan for an organization?

How can documenting disaster recovery procedure improve the success of the organization in the event of a disaster?

In this paper a FCM is utilized to perform risk and scenario analysis for understanding vulnerabilities of a disaster recovery plan model. Next section utilizes the proposed FCM to perform simulation to assess risk using what-if scenario analysis for the FCM disaster recovery plan model as shown in Figure 9. Using what-if scenario analysis managers and decision makers can identify and rectify problems.

4 Simulation

Consider the following scenario: What are the effects of improving personnel training for disaster recovery?

This situation can be presented using vector I_0 = [0, 1, 0, 0, 0, 0, 0]. In vector I_0 the concepts improving personnel training is represented as the second element (concepts C2 based on the FCM as shown in Figure 9 and Table 1) in this vector. Therefore C2 is set to 1 and all other elements are set to zero representing that the other concepts have yet to take place. It is assumed that C2 occurs and no other concepts have occurred at the moment. A FCM can be used to identify and access risks that may arise due to unavailability or shortcomings of different concepts for a given organization.

Now I_0*E can provide the solution for this situation as follows: I_0*E = [0.5, 0, 0, 0.6, 0, 0, 0.6] = I_1 which concludes that if C2 happens then it influence and increase the possibility of success in C1, C4 and C6. We apply the threshold function to I_1 with threshold value set to 0.5. That is I_0*E = [1, 0, 0, 1, 0, 0, 1] = I_1 Continuing I_1*E = [0.5, 0, 0, 1.2, 0, 0, 0] = I_2. Now we apply the threshold function to I_2 = [1, 0, 0, 0, 1, 0, 0, 0]. This means if C2 happens then C1 and C5 will happen. In conclusion disaster recovery planning will be improved by improving training of disaster recovery personnel. Regardless of the concepts and influence weights used the analysis must precede along the flow of the arcs as indicated by the arrows on FCM model as shown in Figure 9. Other what-if scenario analysis can be performed in similar manner. The following what-if scenarios are performed and the results are shown in Table 2.

Table 1. Matrix E built based on the concepts of the FCM disaster recovery planning model shown in Figure 9

$$E = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.5 & 0 & 0 & 0.6 & 0 & 0 & 0.6 \\ 0.4 & 0 & 0 & 0 & 0.6 & 0 & 0 \\ 0.4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.5 & 0 & 0 & 0 & 0 & 0.6 & 0 \\ 0.5 & 0 & 0 & 0 & 0 & 0 & 0.6 \\ 0.8 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Table 2. Consequences of different scenarios based different what if simulations

Scenario No	What if the event occurs	Consequences
1	C2, C4, C5	C2, C4, C5 ⇒ C1
2	C5, C6	C5, C6 ⇒ C1
3	C7, C3	C7, C3 ⇒ C1
4	C3	C3 ⇒ C5 ⇒ C6 ⇒ C7 ⇒ C1
5	C5	C5 ⇒ C6 ⇒ C7 ⇒ C1
6	C3	C3 ⇒ C5 ⇒ C1
7	C6	C6 ⇒ C1 and C6 ⇒ C7 ⇒ C1

Scenario 1: What happens if training of disaster recovery (C2) staff is improved and the role of these staff across department (C4) are established and polices (C5) are improved?
Scenario 2: What are the effects of improving policies (C5) and documenting disaster recovery procedures (C6)?
Scenario 3: How preparedness (C7) of an organization for disaster recovery planning and assessing all risks (C3) in an organization assist an organization?
Scenario 4: What are the effects of establishing roles (C3) and preparedness in improving continuity in an organization operation when a disaster strikes?
Scenario 5: What are the effects of improving disaster recovery planning polices (C5)?
Scenario 6: What are the effects of accessing risk (C3) and identifying risk in improving recovery polices (C5)?
Scenario 7: What are the effects of improving and documenting disaster recovery procedures?

Managers and decision maker can use the information provided from the what-if scenarios for the FCM disaster recovery planning model for risk analysis. A large number of what-if scenarios can be performed easily and accurately and the result of each what-if scenario can be evaluated using the FCM disaster recovery planning model immediately and quickly.

5 Conclusion

Managing and monitoring disaster recovery plans are becoming increasingly difficult and as such many disaster recovery management techniques can become flawed. Existing disaster recovery planning and management techniques do not provide complete facilities to analyse and assess different risks that may exist in such models in a systematic way.

This paper considers the implementation of a Fuzzy Cognitive Maps (FCM) to provide facilities to capture and represent complex relationships in a disaster recovery planning and management models to improve the understanding of CIO's, managers and other personnel involved about their disaster recovery plan and associated risks in their organization. In this paper a FCM disaster recovery planning and risk assessment model is considered using disaster recovery concepts used in [1]. There are a large number of concepts in the FCM disaster recovery planning and assessment model. Fuzzy Cognitive Maps (FCM) is employed in this paper to provide facilities to capture and represent complex relationships in the proposed disaster recovery model to improve the understanding of CIO's, managers and decision makers to analyse risks in this model. Different scenarios are considered using the proposed FCM disaster recovery model. By using the proposed model, a disaster recovery plan can regularly be monitored, reviewed and improved. Decision makers can perform what-if analyses to better understand vulnerabilities and pitfalls in their disaster recovery plan.

References

1. Erbschloe, M. Guide to Disaster Recovery, Thomason Course Technology, (2003)
2. Anderson, J. New trends in backup: Is your disaster recovery plan keeping up? The eSecurity Advisor, 8, 2, pp. 58, (2008)
3. Baker, S. Lessons learned: A devastating hurricane caused this CIO to rethink his carrier's disaster recovery plans, Tech Decisions, Volume 3, Number 10, pp. 30, (2008)
4. Beaman, B. Albin, B.. Steps to disaster recovery planning, Network World, Volume 25, 6, (2008)
5. Kosko, B. Fuzzy Cognitive Maps, International Journal of ManMachine Studies, Vol 24, pp. 65-75, (1986)
6. Andreou, A.S., Mateou, N.H., Zombanakis, G.A. Evolutionary Fuzzy Cognitive Maps: A Hybrid System for Crisis Management and Political Decision Making, Proceedings of the International Conference on Computational Intelligence for Modelling, Control and Automation, (2003)