5th SASTech
Iran | Mashhad
May 12 - 17 | 2011
5th Symposium on Advances in Science & Technology

Study on Immune System of human body and its relationship with Risk Management in organizations

Azadeh Sarkheyli
Department of Information Systems
M.S. Student of University of Technology Malaysia (UTM)
sarkheyli@yahoo.com

Norafida binti Ithnin
Department of Computer System & Communication
University of Technology Malaysia (UTM)
Johor Bahru, Malaysia
afida@utm.my

Arezoo Sarkheyli
Computer Engineering Department
Payam Noor University
Tehran, Iran
arezo_sarkheyli@yahoo.com

Paper Reference Number: 871
Name of the Presenter: Arezoo Sarkheyli

Abstract

Human body has the natural ability to protect and heal itself, like all the systems which existing in the nature. It means that, Immune System which is one of the main systems in humans that protects them from illness. In other words, it is a network of cells, tissues, and organs designed complexly for preventing the body against germs, viruses, and other form of body toxins. As microbial invasions attempt to pass through the body's natural barriers, immune system alerts body's defenses and calls to action the natural processes that keep the body safe and healthy.On the other hand, Risk Management in the organizations includes the processes concerned with identifying, analyzing and evaluation the factors that might adversely affect project outcomes which is important as one of the main items in security management. Because of these many methodologies are created for risk management, but some failures are specified in these methodologies. In other words, they are not complete. Hence the research wants to find a relationship between Immune System as one of the complete management systems in nature, and current methodologies of risk management, by comparison of them with each other.
However the findings of this study are important to help organizations toward improving Risk Analysis process by investigation about Immune System activity and current procedures of Risk Management methodologies. So the information in this paper could be published and more extensive studies could be planned for the future.

Keywords _ Risk Analysis/Management, Immune System, risks/attacks, Risk Management Methodology

1. Introduction

There are a lot of methodologies as Risk Management which are created for identifying, analyzing risk and manage them but existing evidence show that these models are not complete in order to manage risks correctly. So the importance of risk management and entity of complete systems in the nature cause the study wants to find a relationship between them. It means that Risk Management process in current situation of organizations and Immune System as one of the complete system in the nature. Hence the study tries to propose a new process of risk management by investigation on the existing methodologies, and Immune System activities via simulation the processes of it.

Anyway this paper consists of research in Immune System which will be described initially, after that the definition of risk management, then some of the existing methodologies of risk management that are selected in this investigation will be discussed and comprised. Following that, the last description is the steps of Immune System that will be studied. Finally a process of risk management will be proposed.

2. Research in Immune System

In this study tries to propose a new description of IT Risk Management process using the relationship of it with Immune System, because of this Immune system as the main system, which this research wants to investigate base of it, will be described in this part.

Undoubtedly immune system is a complex network of cells, tissues, and organs designed to defend the body against germs, viruses, and other form of body toxins. As microbial invasions attempt to pass through your natural barriers, your immune system alerts your body's defences and calls to action the natural processes that keep you safe and healthy (Mohler and Barton, 2007).

Like nature, your body has the natural ability to protect and heal itself. This happens through your immune system. Research shows a healthy immune system helps prevent most common illnesses. Mohler, Barton(2007) mentioned that strengthening your immune system could be increases body ability to defend from invasive microbes, strengthens body's response to pathogens, shortens infection times and allows for quick healing, enhances vitality a feeling of well-being, improves overall health and quality of life.

Immune system contains of two parts, it means that Acquired Immune System and the Innate Immune System. Obviously each of these has a specific role in defending the body; hence there are major differences between them. On one hand, innate immune system is always working; it means that it used to protect the body and does not require any special preparation to stop infection. On the other hand, acquired immune system as clear as the name of it, needs to be primed before it can work to its full effectiveness though, and is only really effective after it has seen a possible infective agent before (Dasgupta, 1999). In summary, innate immune system and acquired immune system are shown in Fig2 (Dasgupta, 1999); because of this the difference between them is clear.

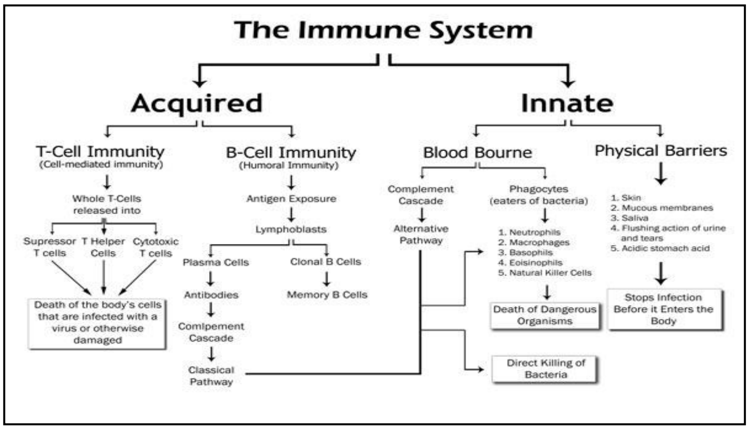


Fig2: Immune System diagram

The process of Immune system is divided to three lines of defences. In other words, First line as the initial defences could be a public defences against the risks existing in the environment, this bar is related to innate immune system which is always working and it used to protect the body and does not require any special preparation to stop infection, so another barrier is related to second and third line of defences. About the second line of defences, it can represent that also this line is related to innate immune system like the firs bar. Hence specific preparation does not necessary for doing its task. The other is close to acquired immune system which needs to be primed before it can work to its full effectiveness though, and is only really effective after it has seen a possible infective agent before (Harmer, 2002 and Hedberg, *1996*). However the process of immune system listed in below as three lines of barrier that are mentioned.

First-line Defenses consist of defense against pathogens uses mostly physical and chemical barriers and prevention or destroy the pathogens. Then Second-Line Defenses which is consist of identify the pathogens, inflammatory response for killing the pathogens, this is a reaction that causes redness, heat, swelling, and pain in the area of infection and destroy the pathogens and recovery. Finally, Third-Line Defenses that includes of determines between kinds of pathogens. For each type of pathogen, produces cells that are specific for that particular pathogen, destroy the pathogens and recovery and remembers each foreign substance and pathogen that enters the body.

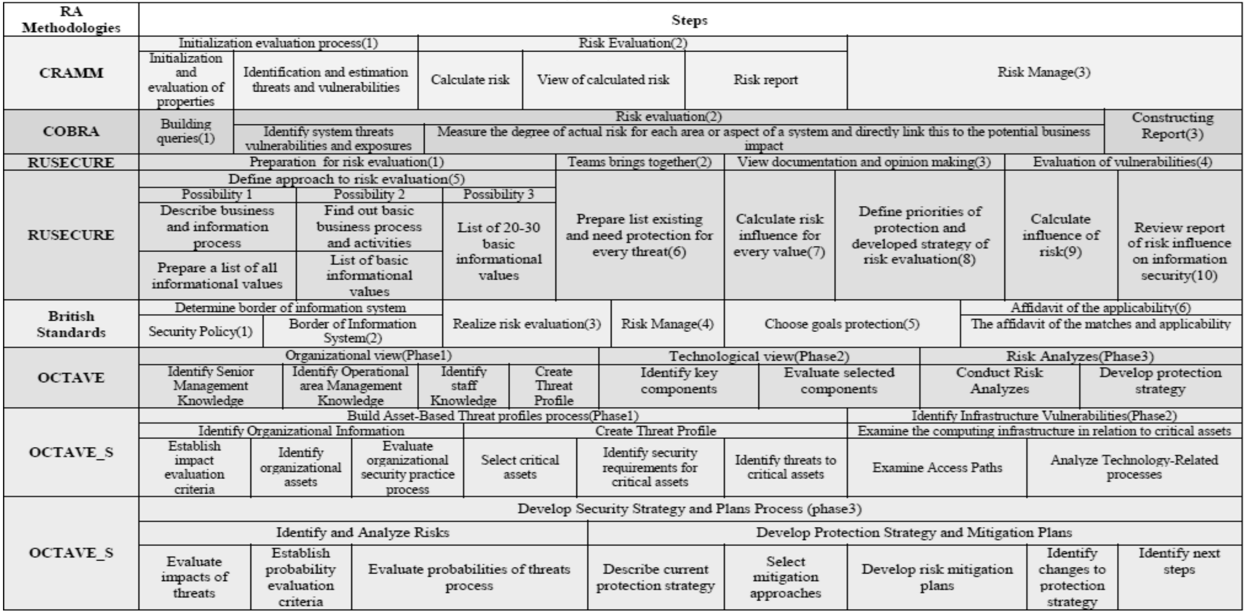
3. Risk Management

Risks to a company could be happen in different forms, and they are not all computer related. Any way this study wants to focus on IT/IS risk management. Then in that case information risk management is the process of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain that level.

Every environment has vulnerabilities and threats to a certain degree. The skill is identifying these threats, assessing the probability of them actually occurring and the damage they could cause, after that taking the right steps for reducing the overall level of risk in the environment to what the organization identifies as acceptable. A risk analysis could identify assets of the company, discover the threats that put them at risk, and also can estimate the possible damage and potential loss a company could be stable if any of these threats becomes real. The results of the risk analysis could be benefit in management construct a budget with the necessary funds as protection the recognized assets from their identified threats and develop security policies which could provide direction for security activities. Risk analysis has three main steps which are asset and information value assignment as step1 after that risk analysis and assessment as step2 and the last step is countermeasure selection and implementation(Harris, 2008). Eventually, for the risks associated with information and information technology (IT) to be identified and managed cost-effectively, it is necessary that the process of analyzing and assessing risk is well understood by all parties and executed on a timely basis. After that risk assessment is for characterization of the process and the result of analyzing and assessing the risk (Siong Neo, 1994). Although the term of Risk Management has various descriptions, they are same. In other words the difference between various methodologies is related to their process. Generally the total process of risk management has five or six steps as present in general description of risk management

4. Risk Management Methodologies

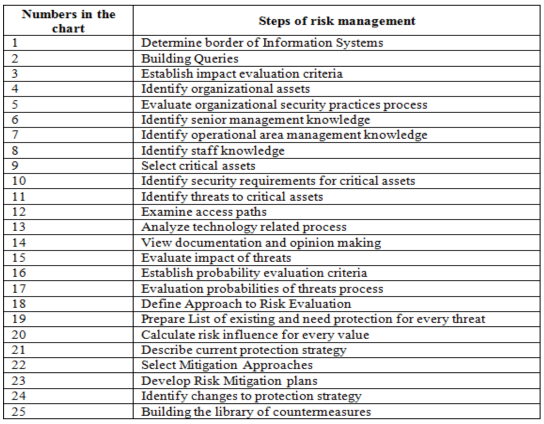
As mentioned in the previews part, several methodologies for managing the risk which are designed for the organizations are selected in this study. Table1 shows the process of the methodologies which have chosen in this investigation. So the steps of these methods for simply comparisons and study are gathered as a table. So COBRA, CRAMM, RUSECURE, British Standards, OCTAVE and OCTAVE-S are risk analysis methodologies as it mentioned before are shown in the created table. These tables show all steps of the methodologies specifying in their own row, consequently their phases consider with their own number, phase1, phase2 and phase3 for example.Table1(Boehm, B.W., (1991), Woody(2006), Caralli(2007), Stoneburner(2002), ARMY(2001), Michael(2002), Alberts(2003), Henley(1996), Januszkiewicz(2007), Maglogiannis(2006)) shows as below:



RA Methodologies	Steps							
CRAMM	Initialization evaluation process(1)		Risk Evaluation(2)			Risk Manage(3)		
	Initialization and evaluation of properties	Identification and estimation threats and vulnerabilities	Calculate risk	View of calculated risk	Risk report			
COBRA	Building queries(1)	Risk evaluation(2)						Constructing Report(3)
		Identify system threats vulnerabilities and exposures	Measure the degree of actual risk for each area or aspect of a system and directly link this to the potential business impact					
RUSECURE	Preparation for risk evaluation(1)			Teams brings together(2)	View documentation and opinion making(3)		Evaluation of vulnerabilities(4)	
RUSECURE	Define approach to risk evaluation(5)			Prepare list existing and need protection for every threat(6)	Calculate risk influence for every value(7)	Define priorities of protection and developed strategy of risk evaluation(8)	Calculate influence of risk(9)	Review report of risk influence on information security(10)
	Possibility 1	Possibility 2	Possibility 3					
	Describe business and information process	Find out basic business process and activities	List of 20-30 basic informational values					
	Prepare a list of all informational values	List of basic informational values						
British Standards	Determine border of information system		Realize risk evaluation(3)	Risk Manage(4)	Choose goals protection(5)		Affidavit of the applicability(6)	
	Security Policy(1)	Border of Information System(2)					The affidavit of the matches and applicability	
OCTAVE	Organizational view(Phase1)				Technological view(Phase2)		Risk Analyzes(Phase3)	
	Identify Senior Management Knowledge	Identify Operational area Management Knowledge	Identify staff Knowledge	Create Threat Profile	Identify key components	Evaluate selected components	Conduct Risk Analyzes	Develop protection strategy
OCTAVE_S	Build Asset-Based Threat profiles process(Phase1)						Identify Infrastructure Vulnerabilities(Phase2)	
	Identify Organizational Information			Create Threat Profile			Examine the computing infrastructure in relation to critical assets	
	Establish impact evaluation criteria	Identify organizational assets	Evaluate organizational security practice process	Select critical assets	Identify security requirements for critical assets	Identify threats to critical assets	Examine Access Paths	Analyze Technology-Related processes
OCTAVE_S	Develop Security Strategy and Plans Process (phase3)							
	Identify and Analyze Risks			Develop Protection Strategy and Mitigation Plans				
	Evaluate impacts of threats	Establish probability evaluation criteria	Evaluate probabilities of threats process	Describe current protection strategy	Select mitigation approaches	Develop risk mitigation plans	Identify changes to protection strategy	Identify next steps

Table 1. Risk Management methodologies process.

Consequently viewing the hole of methodologies in one table and comprising them with each other could be the result of this table. So some steps which are common between them are clear, such as Identify threats to critical assets which are the same for all of them or Evaluate Impacts of threats is common between all of them expect of OCTAV and so on. Hence a chart as Fig3 is created for comparison the methodologies steps that is one of the main factors for specification of strengths and a weakness of them that is shown as below.



Numbers in the chart	Steps of risk management
1	Determine border of Information Systems
2	Building Queries
3	Establish impact evaluation criteria
4	Identify organizational assets
5	Evaluate organizational security practices process
6	Identify senior management knowledge
7	Identify operational area management knowledge
8	Identify staff knowledge
9	Select critical assets
10	Identify security requirements for critical assets
11	Identify threats to critical assets
12	Examine access paths
13	Analyze technology related process
14	View documentation and opinion making
15	Evaluate impact of threats
16	Establish probability evaluation criteria
17	Evaluation probabilities of threats process
18	Define Approach to Risk Evaluation
19	Prepare List of existing and need protection for every threat
20	Calculate risk influence for every value
21	Describe current protection strategy
22	Select Mitigation Approaches
23	Develop Risk Mitigation plans
24	Identify changes to protection strategy
25	Building the library of countermeasures

Table2: Legend of Fig3

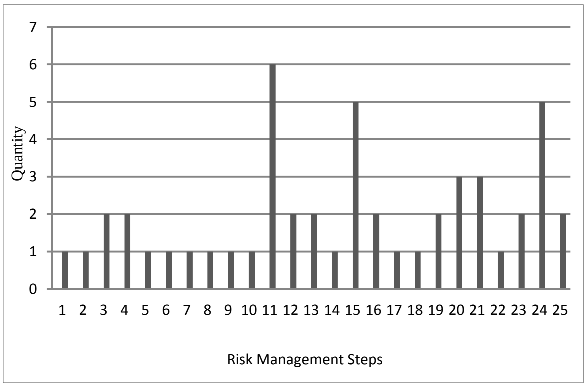


Fig3: Comparing the Steps of Risk Management Methodologies

5. Results and Analysis

The data and information about risk management and Immune System gathered in the previous sections. Hence in this part the process and activity of immune system will be described by creating a table and will be comprised with a process of risk management. Fig4 is created in this study because it wants to be a model for risk management that it is mentioned before. Hence three lines of barrier are specified in this flowchart, it means that, before the first condition there is first line of defence after that there is the second line of defence. If these barriers could not be successful in their task, specific function will be created for protection and recovery of system from the existing risk. So fig4 will be shown below.

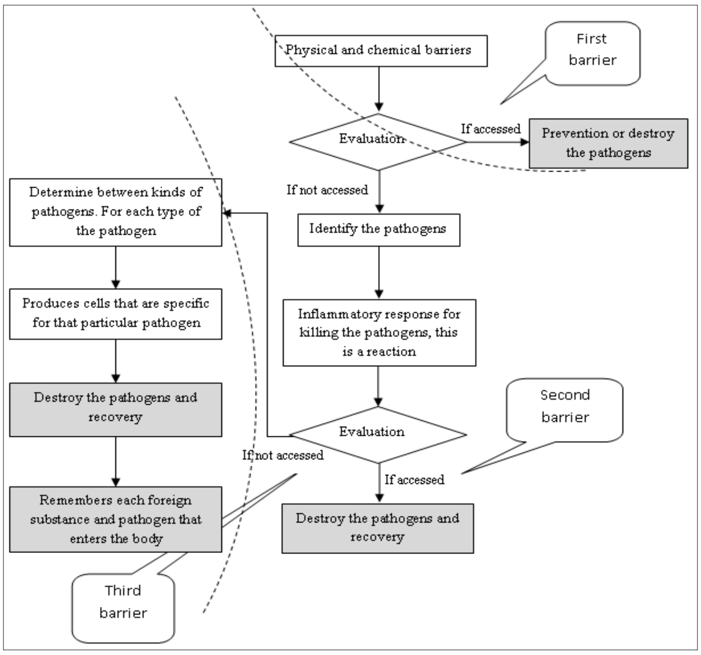

Physical and chemical barriers
First barrier
Evaluation
If accessed
Prevention or destroy the pathogens
If not accessed
Identify the pathogens
Determine between kinds of pathogens. For each type of the pathogen
Produces cells that are specific for that particular pathogen
Inflammatory response for killing the pathogens, this is a reaction
Destroy the pathogens and recovery
Evaluation
Second barrier
If not accessed
If accessed
Remembers each foreign substance and pathogen that enters the body
Destroy the pathogens and recovery
Third barrier

Fig4: Flowchart of the Immune System activity

However, Immune system process and the current process of risk management (a general process of existing Risk Management methodologies) should be comprised; because of this a table is created in order to comprise their process. Obviously there are three barriers in the Immune System process; on the other hand risk management process will be shown in comparison with these lines of defences existing in immune system. So Table3 is created for presenting it:

	First-line Defenses		Second-Line Defenses			Third-Line Defenses			
The Process of Immune System	Body's first line of defense against pathogens uses mostly physical and chemical barriers	Prevention or destroy the pathogens	Identify the pathogens	Inflammatory response for killing the pathogens. This is a reaction that causes redness, heat, swelling, and pain in the area of infection.	Destroy the pathogens and recovery	Determines between kinds of pathogens. For each type of pathogen	Produces cells that are specific for that particular pathogen.	Destroy the pathogens and recovery	Remembers each foreign substance and pathogen that enters the body.
The Process of Risk Management	Uses current controls	Prevention or destroy the risks	Identify the hazards	Proposes planned controls	Develop Initial Security Strategies Identify Infrastructure Vulnerabilities Develop Security Strategy and Plans	None	None	None	Record your findings and implement them Review your assessment and update if necessary

Table 3: Comparison of the Immune system process with the current process of Risk Management

In this investigation has tried to propose a new description of risk management process. Hence because of the differences existing between them as Table 3 shows that, relevant processes for each line of barriers as similar as Immune System barriers will be created. Consequently, aggregation of data and information should be done initially and Information Asset Table, Threat/Attack Profile Table and Control Table are the result of this phase that Fig5shows it as below.

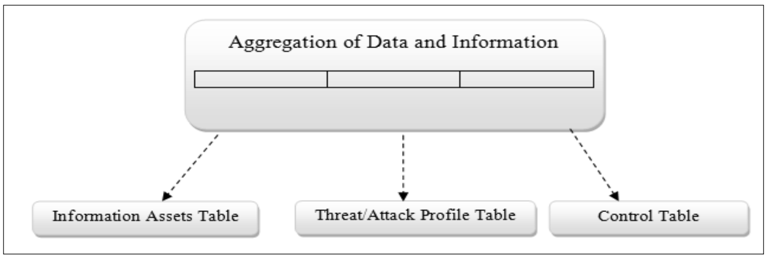

Aggregation of Data and Information
Information Assets Table
Threat/Attack Profile Table
Control Table

Fig5: Aggregation of Data and Information phase and the outputs of it

Fig6, Fig7 and Fig8 are created based on the first, second and third lines of barrier respectively that are existing in Immune System. Fig6 shows that Information Asset Table, Threat/Attack Profile Table and Control table are the inputs of the process, and then risk could be identified based on these tables and risk level matrix. If there is not any risk in the organization, it represents that current controls implementing in the organization are suitable and the first line of barrier is successful, so the process will be done. On the other hand if there is any risk in the organization, it shows that the second line of barrier must be active for avoiding the risk by identify new risks as Fig6 shows that.

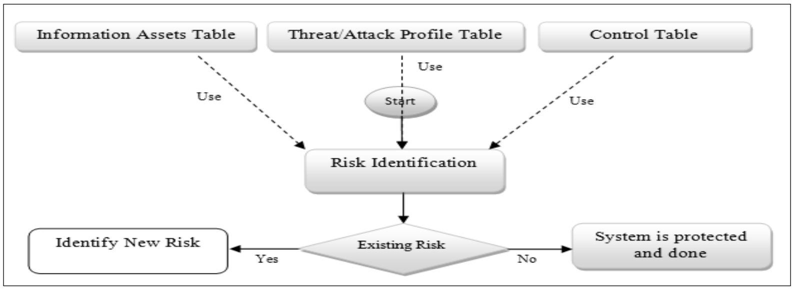


Fig6: Flowchart of first line of barrier

Fig7 represents the second line of barrier of the risk management process. Hence planned controls which are accumulation by analysers or security specialists could implement in this phase. After reaction and recovery, risk should be evaluated again as Fig7 shows it in the existing risk condition. Then if there is not any risk in the organization, the process will be finished. If there is any risk yet, the third barrier should be active.

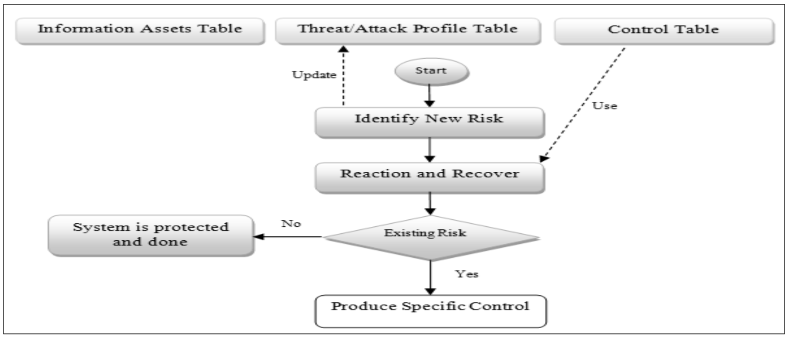


Fig7: Flowchart of the second line of barrier

About Fig8, it shows that the current control and planned control in the Control Table could not sufficient for avoiding the risk, so in this phase a specific control could be product base on the history of risk management which should learn to the system as an intelligence system (Abraham (2005), Fausett(1994)). At the end phase if the process cannot present any solution for management the risk, a new control should be planned by experts. This control will add to the Control Table for the next similar risk.

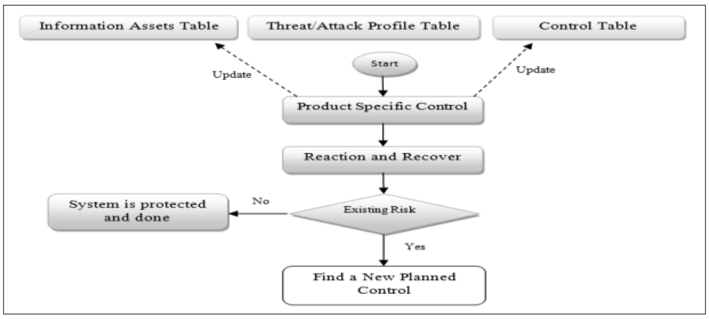


Fig8: Flowchart of the third line of barrier

The lack of specific function which recover/avoid risks/attacks toward IS/IT component in the current methodologies could be the main deference between existing methodologies and this method. So as it is mentioned reaction and recovery, product specific control and update the related table after each step are specific in this method toward improving the performance of risk management. It should mention that the first part of the process is related to innate system that always working. Another part is closed to acquired system that is presented in Fig8. And Fig9 shows all of the process in one flowchart, as the figure below.

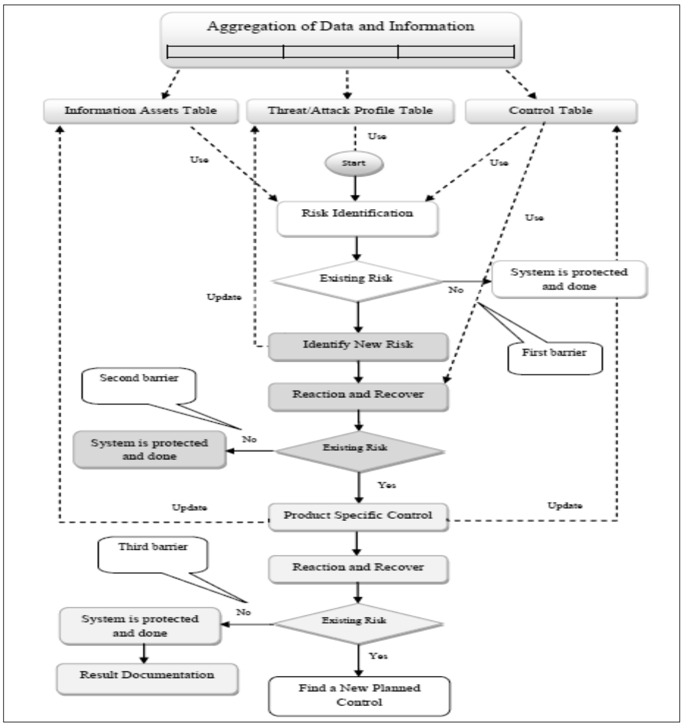


Fig9. Proposed Risk Management Process using Immune System

Immune system process and the offered process of risk management should be comprised again as a result of this study; because of this Table4 is created in order to comprise their process.

	First-line Defenses		**Second-Line Defenses**			**Third-Line Defenses**			
The Process of Immune System	Body's first line of defense against pathogens uses mostly physical and chemical barriers	Prevention or destroy the pathogens	Identify the pathogens	Inflammatory response for killing the pathogens. This is a reaction that causes redness, heat, swelling, and pain in the area of infection.	Destroy the pathogens and recovery	Determines between kinds of pathogens. For each type of pathogen	Produces cells that are specific for that particular pathogen.	Destroy the pathogens and recovery	Remembers each foreign substance and pathogen that enters the body.
The Process of Risk Management	Uses current controls	Prevention or destroy the risks	Identify new risk	Uses planned controls	Reaction, Recovery	Product Specific Control		Reaction, Recovery	Update the Tables, Result Documentation

Table 4: Comparison of the Immune system process with the proposed process of Risk Management

6. Conclusions

In conclusion, the new definition of risk management which is related to this study is risk management includes the processes concerned with identifying, analyzing and responding to those factors these processes divided to three defense bar. It means that after achieving three main table toward Aggregation of Data and Information phase the method tries to defense the organization which is the first barrier then if current controls could not sufficient in defense against the threat/ attach second barrier could be active, consequently third barrier as an acquired part will active if first and second defense barrier as innate parts have not been successful. Anyway, try to develop the process using artificial neural network and test the propose Risk Management process toward specific attacks in the real environment at the end phase of this research is a plan for future work.

References

R. R. Mohler, C.F.Barton. (2007)" Immune system control", Decision and Control including the 14th Symposium on Adaptive Processes, 1975 IEEE Conference on.

D. Dasgupta, Ed., Artificial Immune Systems and Their Applications, Heidelberg, Germany: Springer-Verlag, 1999.

Paul K. Harmer, Paul D. Williams, Gregg H. Gunsch, and Gary B. Lamont," An Artificial Immune System Architecture for Computer Security Applications" , IEEE TRANSACTIONS ON EVOLUTIONARY COMPUTATION, VOL. 6, NO. 3, JUNE 2002

Sara Hedberg. (1996)"Combating computer viruses: IBM's new computer immune system," IEEE Concurrency, vol. 4, no. 2, pp. 9-11.

Shon Harris, "CISSP All-in-One Exam Guide" Fourth Edition, by the McGraw-Hill Companies, 2008.

Boon Siong Neo, Kewong Sin Leong,"Managing Risks in Information Technology Projects" Journal of Information Technology Management, Volume V, Number3,1994

Boehm, B.W., 1991. Software Risk Management: Principles and Practices, IEEE Software, No. 1, pp. 32-41, IEEE CS Press.

Carol Woody_ Carnegie Mellon University, "Applying OCTAVE" is sponsored by the U.S. Department of Defense, May 2006.

Richard A.Caralli, James F.Stevens, William R.Wilson "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process", Software Engineering Institute from Carnegie Mellon University, May 2007

Gary Stoneburner, Alice Goguen, and Alexis Feringa," Risk Management Guide for Information Technology Systems" NIST Special Publication 800-30, 2002.

ARMY, MARINE CORPS, NAVY, AIR FORCE, "Risk ManagementF, february 2001.

Michael A. Greenfield Deputy Associate Administrator Office of Safety and Mission AssuranceLangley Research Center "Risk Management Tools" May 2, 2000

Risk Management Guide for Information Technology Systems, Recommendations of the National Institude of Standards and Technology, 2002.

Christopher Alberts, Audree Dorofee, Carol Woody_ Carnegie Mellon University,"Introduction to the OCTAVE Approach" is sponsored by the U.S. Department of Defense August 2003.

E. Henley, H. Kumamoto(1996). Probabilistic Risk Assessment 2nd edition, IEEE Press, New York.

Paulina, Januszkiewicz ; Marek, Pyka ;” Designing a Security Policy According to BS 7799 Using the OCTAVE Methodology”, The Second International Conference on Availability, Reliability and Security IEEE. ARES 2007.

Maglogiannis, I.; Zafiropoulos, E.;” Modeling Risk in Distributed Healthcare Information Systems”, Engineering in Medicine and Biology Society. EMBS '06. 28th Annual International Conference of the IEEE, 2006.

Artificial Neural Networks , Ajith Abraham, Oklahoma State University, USA, Handbook of Measuring System Design , 2005, John Wiley and Sons, ISBN: 0-470-02143-8