

**INSIDER THREAT RISK MANAGEMENT FRAMEWORK**

**MOHD HAFIZ BIN MOHD AMABR**

**UNIVERSITI TEKNOLOGI MALAYSIA**

# INSIDER THREAT RISK MANAGEMNET FRAMEWORK

MOHD HAFIZ BIN MOHD AMBAR

A project report submitted in partial fulfillment of the  
requirements for the award of the degree of  
Master of Computer Science (Information Security)

Faculty of Computer Science and Information Systems  
Universiti Teknologi Malaysia

AUGUST 2012

## ACKNOWLEDGEMENT

First and foremost, I want to thank to the Almighty Allah who gave me the strength to do this thesis. Allah give me the courage and hope for me to go through everything to end this thesis.

Secondly, i would like to express heartfelt gratitude to my supervisor Dr.Norafida Bt Ithnin for their constant support during my study at UTM. They inspired me greatly to work in this project. Willingness to motivate me to contribute tremendously to my project was outstanding. I have learned a lot from them and i am fortunate to having them as my mentor.

Besides that, i would like to thank the authority of Universiti Teknologi Malaysia (UTM) for providing me with a good environment and facilities such as Computer laboratory to complete this project with software which I need during process.

## ABSTRACT

In an organization which is actively involved in administrative or management work, data is the most valuable asset. Without proper preparation and adequate knowledge, those asset will be exposed at high risk to threat. Office of Student Affairs is the main office of the university management. It handled a lot of sensitive data and information that can be manipulated by unscrupulous people for personal gain. Any negative impact on the information can affect an organization's operations and organizational performance. The most worrying threat is caused by the insiders themselves. Threats from people inside can be specified to both technical and non technical. This problem is difficult to overcome but with the effective measures can reduce this risk to a greater minimum. Implementing risk management framework into the organization a good alternative. By creating a framework for information security that specific to an organization can help reduce this problem by deliver a practical guideline for everyday practices. The processes to produce this framework are going through selecting common feature available in existing framework. Exiting framework process was merging depending on the selected feature and threat to produce a framework that focus on UTM office of Student Affair. Those risk management framework design were specific for UTM office of Student Affair work flow by aiding and assist the organization towards securing their data confidentiality, integrity and availability.

## ABSTRAK

Dalam sesebuah organisasi yang terlibat secara aktif dalam kerja-kerja pentadbiran atau pengurusan, data adalah aset yang paling berharga. Tanpa persediaan yang betul dan pengetahuan yang mencukupi, aset mereka akan terdedah pada risiko yang tinggi kepada ancaman. Pejabat Hal Ehwal Pelajar adalah pejabat utama pengurusan universiti. Ia mengendalikan banyak data yang sensitif dan maklumat yang boleh dimanipulasi oleh orang-orang yang tidak bertanggungjawab untuk keuntungan peribadi. Sebarang kesan negatif ke atas maklumat yang boleh menjejaskan operasi organisasi dan prestasi organisasi. Ancaman yang paling membimbangkan adalah disebabkan oleh orang dalaman itu sendiri. Ancaman daripada orang dalam boleh dikelaskan kepada dua iaitu teknikal dan tidak teknikal. Masalah ini sukar untuk diatasi tetapi dengan langkah-langkah yang berkesan dapat mengurangkan risiko ini ke tahap yang lebih minimum. Melaksanakan rangka kerja pengurusan risiko ke dalam organisasi satu alternatif yang baik. Dengan mewujudkan satu rangka kerja bagi keselamatan maklumat yang khusus kepada sesebuah organisasi boleh membantu mengurangkan masalah ini dengan memberikan satu garis panduan yang praktikal untuk amalan harian. Proses untuk menghasilkan rangka kerja ini ialah melalui pemilihan ciri biasa yang ada dalam rangka kerja yang sedia ada. Proses rangka kerja sedia ada akan digabungkan yang bergantung kepada ciri-ciri dan ancaman yang dipilih untuk menghasilkan satu rangka kerja yang memberi fokus kepada pejabat UTM Hal Ehwal Pelajar. Rekabentuk rangka kerja pengurusan risiko ini adalah khusus untuk cara kerja pejabat Hal Ehwal pelajar UTM dengan membantu dan membimbing organisasi ke arah melindungi kerahsiaan, integriti dan ketersediaan data.

## TABLE OF CONTENT

<b>CHAPTER</b>	<b>TITLE</b>	<b>PAGE</b>
	<b>DECLARATION</b>	ii
	<b>ACKNOWLEDGEMENTS</b>	iii
	<b>ABSTRACT</b>	iv
	<b>ABSTRAK</b>	v
	<b>TABLE OF CONTENTS</b>	vi
	<b>LIST OF TABLES</b>	xii
	<b>LIST OF FIGURES</b>	xiv
	<b>LIST OF ABBREVIATION</b>	xvi
	<b>LIST OF APPENDIX</b>	xvii
<b>1</b>	<b>INTRODUCTION</b>	
	1.1 Introduction	1
	1.2 Problem Background	2
	1.3 Problem Statement	5
	1.4 Project Aim	6
	1.5 Project Objective	6
	1.6 Project Scope	6
	1.7 Organization of Report	7
	1.8 Summary	8
<b>2</b>	<b>LITERATURE REVIEW</b>	9
	2.1 Introduction	9
	2.2 Introduction to Security	9
	2.3 Introduction to Information Security	11

2.4	Characteristic of Information	12
2.4.1	Confidentiality	13
2.4.2	Integrity	14
2.4.3	Availability	15
2.5	Component of Information Security	16
2.5.1	Hardware	16
2.5.2	Software	17
2.5.3	Data	17
2.5.4	People	18
2.5.5	Procedure	18
2.5.6	Network	19
2.6	Introduction to Threat	20
2.7	Introduction to Human Threat	20
2.7.1	Hacker and Cracker	21
2.7.2	Computer Criminal Threat	22
2.7.3	Terrorist Threat	23
2.7.4	Competitor and Outsider	23
2.7.5	Insider Threat	24
2.8	Technical Insider Threat	26
2.9	Non-technical Insider Threat	27
2.10	Introduction to HEMA	27
2.10.1	Organization Structure	28
2.11	Threat analysis through HEMA	31
2.12	ISO 27000 series (International Standard)	45
2.13	Introduction to Security Framework	47
2.13.1	OCTAVE (J Albert <i>et al</i> ,2001)	50
2.13.2	CORAS (Bjorn Axel Gran <i>et al</i> ,2002)	52
2.13.3	CRAMM (SANS Institute InfoSec Reading room,2012)	55
2.13.4	FAIR (Jack ,2007)	58
2.13.5	NIST RMF (NIST Computer Security Division,2010)	59
2.13.6	TARA (Intel Program IT, 2009)	62
2.13.7	ISRAM (B. Karabacak and I.	64

	Sogukpinar,2003)	
	2.13.8 COBIT (IT Government Institute, 2007)	66
	2.13.9 IS(Bomil Suh and Ingoo Han,2003)	70
2.14	Existing Framework Analysis	72
	2.14.1 Framework Comparison	72
2.15	Summary	75
<b>3</b>	<b>RESEARCH METHODOLOGY</b>	<b>76</b>
3.1	Introduction	76
3.2	Research Roadmap	76
3.3	Phase 1 : Analysis Risk and Framework	80
	3.3.1 Pre-study Phase	81
	3.3.2 Survey Technique	81
	3.3.3 Questionnaire	82
	3.3.4 Interview	84
	3.3.5 Statistical	84
3.4	Phase 2 : Framework Design	85
3.5	Phase 3 : Analysis and validation phase	85
3.6	Summary	86
<b>4</b>	<b>ANALYSIS AND DESIGN</b>	<b>87</b>
4.1	Introduction	88
4.2	Information for framework design	88
4.3	Risk Management Framework for Insider Threat Design Process	89
	4.3.1 Process 1 : List of Features	91
	4.3.2 Process 2: Phase separation process	91
	4.3.3 Process 3: Assessment phase domain categorization	98
	4.3.4 Process 4: Implement Phase domain characterization	101
	4.3.5 Monitor Phase domain categorization	104
4.4	Propose Risk Management Framework For Insider Threat	104



4.5	Assessment Phase Description	106
4.5.1	Identify Asset	106
4.5.2	Valuing Asset	107
4.5.3	Identify Scenario	107
4.5.4	Planning and organize	108
4.5.5	Risk Evaluation	110
4.5.6	Obtain result	110
4.6	Implement Phase Description	112
4.6.1	Assess Acceptance Risk	112
4.6.2	Information Structure	113
4.6.3	Align Strategy by selecting achievement	114
4.6.4	Deliver and support	114
4.7	Monitor Phase Description	116
4.7.1	Monitoring	116
4.7.2	Report	117
4.8	Summary	117
<b>5</b>	<b>RESULT AND ANALYSIS</b>	118
5.1	Introduction	118
5.2	Validation Personal	118
5.3	Expert Validation	119
5.3.1	CICT UTM (Expert 1)	120
5.3.1.1	Expert 1 Assessment Validation	120
5.3.1.2	Expert 1 Implement Validation	121
5.3.1.3	Expert 1 Monitor Validation	121
5.3.1.4	Expert 1 Overall framework process validation	121
5.3.1.5	Expert 1 conclusion	122
5.3.2	ICT UTHM (Expert 2)	122
5.3.2.1	Expert 2 Assessment	122

	Validation	
	5.3.2.2 Expert 2 Implement Validation	123
	5.3.2.3 Expert 2 Monitor Validation	123
	5.3.2.4 Expert 2 Overall Framework Process Validation	124
	5.3.2.5 Expert 2 conclusion	124
5.4	Organization Validation (Office of student Affair)	124
5.4.1	UTM Office of Student Affair	125
5.4.1.1	UTM Office of Student Affair Assessment Validation	125
5.4.1.2	UTM Office of Student Affair Implement Validation	125
5.4.1.3	UTM Office of Student Affair Monitor Validation	126
5.4.1.4	UTM Office of Student Affair Overall framework Operation Validation	126
5.4.1.5	UTM Office of Student Affair conclusion	126
5.5	Risk Management Framework Enhancement	127
5.5.1	Assessment Phase Enhancement	129
5.5.2	Implement Phase Enhancement	131
5.5.3	Monitor Phase Enhancement	132
5.5.4	Overall framework process	133
5.6	New Risk Management Framework Design	134
5.7	Summary	136
<b>6</b>	<b>DISCUSSION AND CONCLUSSION</b>	<b>137</b>
6.1	Introduction	137
6.2	Project Achievement	137
6.3	Project Constraint	138

6.4	Future Works	139
6.5	Summary	139
<b>REFERENCES</b>		141
APPENDIX A-I		147-
		209

## LIST OF TABLE

TABLE NO.	TITLE	PAGE
2.1	Security Multi Layer (Michael E. Whitman & Herbert J. Mattord, 2007)	10
2.2	Information Threat Source Matrix	33
2.3	Threat that cause from human/people Matrix	35
2.4	Insider threat Matrix	37
2.5	Threat mapping with HEMA	40
2.6	Attack mitigation	41
2.7	Security Control Description (ISO 27002)	45
2.8	OCTAVE Process (J Albert <i>et al</i> ,2001)	51
2.9	CORAS Framework Process (Bjorn Axel Gran <i>et al</i> ,2002)	53
2.10	CRAMM process (SANS Institute InfoSec Reading room,2012)	56
2.11	FAIR Process (Jack ,2007)	59
2.12	NIST Risk Management Framework process (NIST Computer Security Division,2010)	60
2.13	Formula Description (McEvoy and Whitcombe, 2002)	65
2.14	COBIT process (IT Government Institute, 2007)	69
2.15	Flow of Risk Analysis (Bomil Suh and Ingoo Han,2003)	70
2.16	Framework features comparison	73
3.1	Overall research plan	78
3.2	Questionnaire Section (Acahill, survey questionnaire design,2003)	83

4.1	Information	88
4.2	Phase mapping	93
4.3	Assessment phase feature mapping	95
4.4	Implementation phase feature mapping	97
4.5	Monitor phase feature mapping	98
4.6	Assessment features in every domain	99
4.7	Assessment Domain mapping	100
4.8	Implement features in every domain	102
4.9	Implementation Domain mapping	103
4.10	Sample consequence table	111
4.11	Likelihood of threat rating	112
5.1	Validation personal	119
5.2	Assessment phase suggestion	127
5.3	Implement phase suggestion	128
5.4	Monitor phase suggestion	128
5.5	Overall design suggestion	128

## LIST OF FIGURE

FIGURE NO.	TITLE	PAGE
2.1	Research Tree	11
2.2	Human Threat Tree	21
2.3	Technical versus Non-Technical Over Time (CERT Software Engineering Institute)	25
2.4	Financial- Technical versus Non-Technical Over Time (CERT Software Engineering Institute)	26
2.5	UTM HEMA Units	30
2.6	Overall analysis three	31
2.7	Data lost type	44
2.8	Relationship between Risk assessment and risk management by Carol Woody et al, 2001	49
2.9	OCTAVE Framework (J Albert <i>et al</i> ,2001)	51
2.10	CORAS Framework (Bjorn Axel Gran <i>et al</i> ,2002)	53
2.11	CRAMM Framework (SANS Institute InfoSec Reading room,2012)	56
2.12	FAIR Framework (Jack ,2007)	58
2.13	NIST Risk Management framework (NIST Computer Security Division,2010)	60
2.14	TARA framework (Intel Program IT, 2009)	62
2.15	TARA process (Intel Program IT, 2009)	63
2.16	ISRAM process	66
2.17	COBIT Framework (IT Government Institute, 2007)	68
3.1	Roadmap of the Study)	77
3.2	Survey process (Survey fundamental guide, 2011	82

4.1	Framework design process	90
4.2	Risk management layout	91
4.3	Phase and features mapping	98
4.4	Assessment domain mapping result	101
4.5	Implement domain mapping result	103
4.6	Propose Framework	105
5.1	Venn diagram on organization overall security position (source: SAI Global IS awareness survey 2008)	129
5.2	Additional element in Assessment phase	131
5.3	Phase rearrangement in Implement phase	132
5.4	Monitor phase additional feature	133
5.5	Final Risk Management Framework	135

**LIST OF ABBREVIATION**

<b>HEMA</b>	Hal Ehwal Mahasiswa (Office of Student Affairs)
<b>LAN</b>	Local Area Network
<b>DOS</b>	Daniel Off Service
<b>SANS</b>	System Admin, Audit, Networking and Security
<b>UTM</b>	Universiti Teknologi Malaysia
<b>OCTAVE</b>	Operationally Critical Threat, Asset and Vulnerability
<b>CORAS</b>	Model Based Risk Assessment
<b>CRAMM</b>	CCTA Risk Analysis and Management Method
<b>FAIR</b>	Factor Analysis of Information
<b>NIST RMF</b>	National Institute of Standard and Technology Risk Management Framework
<b>TARA</b>	Threat Agent Risk Assessment
<b>ISRAM</b>	Information Security Risk Analysis Method
<b>COBIT</b>	Control Objective for Information and Related Technology
<b>IS</b>	Information Security
<b>ISO</b>	International Standard
<b>OS</b>	Operating System
<b>C</b>	Confidentiality
<b>I</b>	Integrity
<b>A</b>	Availability
<b>CNSS</b>	Committee on National Security Systems



**LIST OF APPENDIX**

<b>APPENDIX</b>	<b>TITLE</b>	<b>PAGE</b>
<b>A</b>	Initial Finding Questionnaire For Student	145
<b>B</b>	Initial Finding Questionnaire For Student Result	150
<b>C</b>	Initial Finding Questionnaire For Staff	160
<b>D</b>	Initial Finding Questionnaire For Staff Result	166
<b>E</b>	Framework Feature Validation	189
<b>F</b>	Framework Feature Mapping	195
<b>G</b>	UTM CICT Validation	200
<b>H</b>	UTHM ICT Validation	202
<b>I</b>	UTM HEMA Validation	205

## **CHAPTER 1**

### **INTRODUCTION**

#### **1.1 Introduction**

Most of the organization in the world has their own valuable asset that they need to protect. This valuable assets are including staff, equipment, documentation, financial and more. At this point, the asset that needs to be concern is information documentation that involving all asset that been mention before. This information need to be protected from threat that comes from inside of organization. The threat can be unintentional due to staff carelessness or intentional for personal gain.

It is important to implement security mechanism into every asset to enforce their confidentiality, availability and integrity. The negative effect on data confidentiality, availability and integrity can cost the organization reputation, financial crisis, management crisis and more disaster. So the implementation of information security generally mean to protect the data from unauthorized access, unauthorized use, disclosure, interruption, alteration, unauthorized assessment, recording and destruction.

## 1.2 Problem Background

According to Ramkumar Chinchani et al, 2005, information confidentiality, integrity and availability are at risk because it is vulnerable to insider threat. Threat from insider was known to be low base rate problem. This kind of attack is hard to predict and protect due to the insider threat perpetrator are user with legitimate and authorization. Many attacks continue to spoil or circumvent authentication by combining stolen or guessed credentials to gain access with backdoors. Given the decline in internal agents, the misuse category had no choice but to go down as well. Social tactics fell a little, but were responsible for a large amount of data loss.

The insider threat is also misperceived. Most of the organization was often to concentrate on the threat from outside or external threat. This happen because the tool are available to aid in finding the vulnerabilities such as security audit tools and modeling technique. Insider threat is hard to measure and lack of tool to overcome the situation. Lastly the threat from inside can give very high impact to organization. Maybe threat from insider was not frequently as attack from outside but it poses higher rate of success because the attack activity it is undetected. The insider have the advantage of accessibility and familiar with their target and security countermeasure in place witch therefore attacks of damaging the security system can be done with only a short or non-existent reconnaissance phase.

Inside the organization, there was a lot off staff with difference kind of responsibility and ability. Internal threat is much deadly compare to outsider threat. This insider can become a threat due to their ability to access information and their knowledge about the organization work flow, security measure and physical condition. To understand and anticipating the risks, the critical threat to information system among insider staff can be divide into two categories which is technical and non-technical staff (Privacy Technical Assistance Center,2011). This component can clarify what kind of threat may occur among technical and non-technical staff. According to Eric Shaw *et al*, 1999, Information technology specialists or technical employee such as operators, programmers, networking engineers and systems

administrators is the person who holds positions of unprecedented importance and trust. Malicious actions on the part of such an insider can have dangerous consequences. That malicious action can show several points about the insider threat to the critical information.

The organization mostly handles important information mostly about staff, financial, timely information about activity and more. The data that being handle in the organization should keep their integrity which is the information contain in the data must be consistent and correct. Data inconsistency can come from variety of way and it can be come from current staff who unintended key in wrong information or from carelessness act. Same problem are also can happen to data availability and confidentiality. Those components were also vulnerable to threat.

According to report from Verizon Risk Team on data breach during in early 2012. They state that the corporate and personal information theft was certainly a central part of the tactics. This re-imagined and re-invigorated specter of “hacktivism” rise to haunt around the world. Cybercriminals sustained to automate and streamline their high-volume method and low-risk attacks against weaker targets. Much fewer repeated, but arguably more damaging, were continued attacks targeting trade secrets, classified information, and other intellectual property .Verizon Data Breach Investigation Report in early 2012 comprise more occasion involving data breach, resulting from more contributors, and represent a wider and more various geographical scope. The compromised records number across these incidents increase drastically back up to 174 million after reaching an all-time low in last year’s report of four million. In fact, in the year 2011 boasts the second-highest data loss total since they started keeping track in 2004.

From traditional way of handling important data, most organization implement systematic way of handling data which is using database system. This technology is hopefully can overcome the problem but this information technology has their own weaknesses. The usage of information technology (IT) to handle those valuable information raise concern about the risk to data associated with weak IT

security that including vulnerability to viruses, malware attacks and compromise of network system and services.

The negative impact of vulnerability exercise that considering both probability and occurrence impact is risk. According to Michael E. Whitman, 2003, knowing the foe faced by information security is the most critical component to defining an information security defense bearing. Routinely publish by press dramatic reports a billion dollar lost to fraud, computer theft and abuse. The survey on computer crime and security by the 2002 computer security Institute/Federal Bureau of Investigation (CSI/FBI) found that 90% respondents been report and documented that they acknowledged financial losses because of the computer breaches, a total of roughly \$455,848, 000 in financial losses, up from \$377, 828,700 reported in 2001.

A comprehensive risk management framework is the answer for the components to work together, instead of having stand alone components and system. The connected risk management framework delivers practical guidance for everyday IT practices and activities, helping users establish and implement reliable, cost-effective IT services. Even though the risk management framework does help to solve an issues involving securing the data, not all organization implement this kind of method. The framework supposes to be design according to the organization needs. Not all organization share same kind off process and face same kind of problem and threat. More research on different risk management frameworks in the literature should be done to suit the requirement needed into the organization.

### 1.3 Problem Statement

The true threat for the organization is come from the inside. The organization was vulnerable to insider threat that can cause to violate information confidentiality, availability and integrity (Ramkumar Chinchani *et al*, 2005). Those entity from inside have the rightful access throughout an organization (Predd *et al*,2008). Other cases that concern employees who take their position such as technical employee, information technology specialist or systems administrator have the advantage of trust for financial gain or even hackers who are employed within the organization caught engaging in unauthorized explorations, and “well-motivated” employees who claim they are acting in the best interest of their organizations (Ramkumar Chinchani *et al*, 2005 and Eric Shaw *et al*, 1999). The threat is hard to detect and hard to protect unless there is prevention mechanism. There is a lot of information security framework build to assist the organization in term of securing their information. But those frameworks were too broad and to general. It not focuses on the organization work flow. One weakness about the framework is narrow focus to a particular area, topic or approach. There is no single framework that can suite all organization. (Robert M. Slide, 2009).

The question listed below is some problem that needs to be concern in this research:

- i. What is the threat from insider?
- ii. What is the insider threat problem?
- iii. How serious is the threat from insider?
- iv. What can the data security framework do in certain organization?
- v. How data security framework can help to prevent risk on important data?
- vi. How the risk management framework performances suit the organization?

## **1.4 Project Aim**

The aim of this project is to implement risk management framework for insider threat by merging existing framework features to improving organization security practices and strategies to avoid any risk to compromise data confidentiality, integrity and availability as the organization valuable assets.

## **1.5 Project Objectives**

To complete this research, the project main objective has been acknowledged and all three objectives are shown as follow:

- i. To identify the risk and threat that possible to be happen in an organization
- ii. To propose the risk management framework for insider threat to improve the data security in the organization
- iii. To validate propose risk management framework whether it applicable and suitable can be apply to the organization.

## **1.6 Project Scope**

Scope of the project was including the areas as shows below:

- i. The research is focus on UTM Office of Student Affair and Alumni (HEMA) as a target organization.
- ii. The research are also concern on HEMA valuable assets which is data
- iii. Survey and interview has been done to all units under HEMA and concentrate on the critical unit that handle most important asset.

- iv. The result from the survey and interview describe the awareness level and the countermeasure that should be take to overcome the risk and vulnerability to the information
- v. To design and implement security measure to HEMA

## **1.7 Organization of the report**

This division of the report is to summarize every chapter that contain in this research report. This report holds six chapters. Each and every chapter describes different kind of information as steps to conclude the whole process of the research.

Chapter 1 is an introduction of the research that give overview of whole research that cover problem background, statement of the problems that need to be concern, research objective and also research scope. This chapter provides understanding about the whole idea of the research

Chapter 2 was review on the understanding of risk management and risk management analysis. This chapter also covers a deep understanding of threat, vulnerability and type of method being used from other researcher in this particular field.

Chapter 3 highlights the research methodology used in the implementation of this project. It describes working flow throughout the whole research to ensure the research is based on current objective.

Chapter 4 gives detail design of the framework. This section also describes the enhancement being implemented in the framework. The enhancement is also explained in detail base on initial finding and literature review.



Chapter 5 is validation process which is the step need to be done to ensure the method working according to the objective. This validation goes through an analysis and the result was discussing the statistical calculation base on the feedback from the organization.

Lastly in Chapter 6, it discusses challenge and constrains of the research and also research conclusion. It also covers a discussion on future research on this project that can be improved or upgrade for upcoming use.

## **1.8 Summary**

In this chapter, it describes a basic understanding about this project before moving any further. All the detail contains in this chapter is used as guides to do more research on complete chapter 2.

## References

- Alhabeeb et al. (2010). *Information Security Threats Classification Pyramid*,
- Abramson, J.J. and Abramson, Z.H. (1999). *Survey Methods in Community Medicine: Epidemiological Research, Programme Evaluation, Clinical Trials (5th edition)*. London: Churchill Livingstone/Elsevier Health Sciences, 1999
- Al Bento . (2007) . Impact Of Security Breach On Firm Performance. Journal of information Technology Management
- Acahill . (2003) . Survey questionnaire design. Fairfax County Department of Systems Management for Human Service.
- Alberts, C And Dorofee, A. (2002). *Managing information security risks, The OCTAVE approach*, Addison Wesley, ISBN 0-321-11886-3
- Bornman and Labuschagne. (2004). A Comparative Framework For Evaluating Information Security Risk Management Methods
- Bjørn Axel Gran et al . (2002) . The CORAS Framework for a Model-Based Risk Management Process
- Bomil Suh and Ingoo Han. (2003) . The IS risk analysis based on a business model. Graduate School of Management, Korea Advanced Institute of Science and Technology, 207-43 Cheongryangri-Dong, Dongdaemun-Gu, Seoul 130-012, South Korea
- B. Karabacak and I. Sogukpinar. (2003) . Information Security Risk Analysis Method.
- C. Onwubiko† and A. P. Lenaghan. (2007). *Managing Security Threats and Vulnerabilities for Small to Medium Enterprises*
- Carl Colwill, Human factors in information security: The insider threat e who can you trust these days, 2010
- Christopher Alberts and Audrey Dorofee . (2001). *OCTAVE Threat Profiles*.

- CERT Software Engineering Institute. (2009). Technical and non technical from insider employee
- Carol Woody et al. (2001). The Operationally Critical Threat, Asset and Vulnerability Evaluation version 2.0 . Carnegie Mellon Software Engineering Institute.
- Department of energy.(2007).Cyber Security Threat Statement
- Dodge,Y. (2003) . The Oxford Dictionary of statistical Term.
- Donald L.Evans. (2004). Standards for Security Categorization of Federal Information and Information Systems. Secretary of US Department of Commerce.
- D.W. Straub and W.D. Nance . (1990) .
- Straub, D.W., and Nance, W.D. (1990) Discovering and Disciplining Computer Abuse in Organizations: A Field Study, *MIS Quarterly*, 14,1, 45-60.
- Dempsey et al . (2011). NIST Special Publication 800-137. Information Security . Computer Security Division.
- Dancho Danchev . (2003) . Building and Implementing a successful Information Security Policy. Window Security
- Edwar Humphreys.(2008). Information security management standards : Compliance, governance and risk management
- Eric Shaw, Keven G.Ruby and Herrold M. Post (1999), The Insider Threat to Information System
- Farahmand et al. (2003). *Managing Vulnerabilities of Information Systems to Security Incidents*
- Fairfax County Department of System Management for Human Services(2003), Survey Questionnaire Design
- Gary Stoneburner, Alice Goguen, and Alexis Feringa. (2004). *Recommendations of the National Institute of Standards and Technology*
- Gregory C. Wilshusen. (2009).Cyber Threat and Vulnerabilities Place Federal Systems at Risk
- Gabriel Weimann.(2005). Cyberterrorism : How Real Is The Threat?
- InforSec Reading Room. SANS Institute.(2012).*Assessing Threats To Information Security In Financial Institutions*

Information technology - Security techniques - Information security risk management, ISO/IEC 27005:2008

Ira S. Winkler et al.(2005). Social engineering: The non-technical Threat to Computing System

Ira S.Winkler.(2009).The Non-Technical Threat To Computing System Information Security. (2011), Keeping your information and computers secure while Online.

Intel Program IT . (2009). Threat Agent Risk Assessment. IT @ Intel White Paper

IT Government Institute. (2007). Control Objective for Information and Related Technology.

Janet Edwards, Martin Gustafsson, Barbro Naslund-Landenmark. (2007). Handbook for vulnerability Mapping

J.Noland. (2011). Risk Assessment for Alerting and Monitoring of the Statewide Microwave Network

Joseph Bonneau and Soren Preibusch. (2010). The password thicket: technical and market failure in human authentication on the web

Jake Kouns and Daniel Minoli . (2010) . Information Technology risk Management in Enterprise Environment. A review of Industry Practices and a Practical Guide to Risk Management Teams.

J. Albert et al. (2001). The Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE). Networked Systems Survivability Program

Jack . (2007) . An Introduction to Factor Analysis of Information Risk (FAIR) . Risk Management Insight.

Kevin Rushing. (2008).*Information Risk Management*

Karen D. Loch, Houston H. Carr, Merrill E. Warkentin. (2007) . Threats to Information Systems: Today's Reality, Yesterday's Understanding

Karen J.Jansen, Kevin G.Corley, Bernard J.Jensen, (2006), E-Survey Methodology

Michael E.Whitman & Herbert J.Mattord. (2007). *Introduction to Information Security*.

Michael E. Whitman. (2004). *In defense of the realm: understanding the threats to information security*

- Moore, R. (2005). *Cybercrime: Investigating High-Technology Computer Crime*. Cleveland, Mississippi: Anderson Publishing.
- Michael E. Whitman. (2002). *Enemy at the Gate: Threats to Information Security*.
- Matthew G Devost. (2005). Current and emerging threat to information system and critical infrastructures
- Michael E. Whitman.(2004).In defense of the realm: understanding the threats to information security
- Mark Wilson and Joan Hash . (2003). *Computer Security: Building an Information Technology Security Awareness and Training Program*. National Institute of Standard and Technology.
- Matt Rosenquist. ( 2009) . Prioritizing Information Security Risks With Threat Agent Risk Assessment. Information Security Strategist. Intel Information Technology Security.
- Nik Zulkarnaen Khidzir et al. (2010). *Critical Threats and Vulnerabilities in ICT Outsourcing*.
- Nataliya B. Sukhai. (2005). *Hacking and Cybercrime*. Atlanta Georgia.
- NIST Computer Security Division (2008), Standard for Security categorization of federal information and information system
- NIST Computer Security Division. (2010) . NIST Risk Management Framework.
- Ornstein, M.D. (1998) . *Survey Research* . Current Sociology
- Power, R. 2002. *CSI/FBI computer crime and security survey*. Computer Security Issues & Trends 8, 1 (2002), 1–24.
- Privacy Technical Assistance Center. (2011).Data Security: Top Threat to Data Protection
- Peter et al.(2005). *A Security Risk Analysis Model for Information Systems*
- Paul Baybutt. (2009). Cyber security vulnerability Analysis: Ab Asset-Based Approach
- Predd, J. et al. (2008). Insider Behaving Badly. IEEE Security and Privacy 6 (4), pp. 66-70.
- Quey-Jen Yeh a,\* , Arthur Jung-Ting Chang.(2007). *Threats and countermeasures for information system security: A cross-industry study*

- R.K. Rainer Jr., C.A. Snyder, H.H.Carr. (1991). *Risk analysis for information technology*, Journal of Management Information Systems 1991, pp. 192–197.
- R. Richardson. (2003) .*CSI/FBI Computer Crime and Security Survey, Computer Security* Institute, 2003<http://www.gocsi.com/> (cited September 20, 2003)
- Rahul Bhasker and Bhushan Kapoor. (2009).*Information Technology Security Management*
- Ramkumar Chinchani, Anusha Iyer, Hung Q. Ngo, Shambhu Upadhyaya (2005), *Toward A Theory of Insider Threat Assessment*. University at Buffalo NY USA.
- Rose Tsang , *Cyberhreat, Vulnerability and attacks on SCADA Network*, Rose Tsang, 2010
- Rex Kelly Rainer, Jr., Charles A, Snyder and Houston H.Carr. (2007) . *Risk Analysis for Information Technology*
- Robert M. Slide. (2009) . *Security Framework*
- Ron Kosena.(2011) . *Risk Assessment For Alerting And Monitoring Of The Statewide Microwave Network*. Department of Administration State Information Technology Services Division.
- Steve elky. (2006). *An introduction to information system Risk Management*
- Straub, D.W. and Welke, R.J. (1998). *Coping with systems risk: Security planning models for management decision making*. MIS Q. 22, 4 (1998), 441–469.
- SANS Institute. (2012) . *Assessing Threats To Information Security In Financial Institutions*.
- SAI Global. (2008) . *Information Security Awareness Survey*.
- Timothy Casey. (2007). *Threat Agent Library Helps Identify Information Security Risk*
- Thomas w. Malone ,How . (2000). *Do People Organize Their Desk*
- The Sun Certified Security Administrator. (2005) . *Fundamental Security Concept*. Solaris Operating system exam modules.
- United State Code. (2012) . Title 44 : Public Printing and Document. Coordination of Federal Information Policy
- U.S Government Accountability Office. (2009)

Verizon risk team.( 2012). Data breach investigation report

Wesley Cornelissen. (2009) . Investigating Insider threat : Problem and Solution. Business administration, information management. University of Twente.