Journal of Theoretical and Applied Information Technology
20th December 2014. Vol.70 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

INTERNAL THREAT CONTROL FRAMEWORK BASED ON INFORMATION SECURITY MANAGEMENT SYSTEM

[1]ZAILAWANI MUKHTAR, [2]KAMSURIAH AHMAD
Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, UKM
E-mail: [1]zailawani05@gmail.com, [2]kamsuriah@ukm.edu.my

ABSTRACT

This paper focuses on proposing a framework for security control that based on ISO 27001 and ISO 27002, which is a standard of Information Security Management System (ISMS). This framework helps to mitigate internal threats for data centre meant for public sector adoption. The ISMS implementation scope in the public sector normally comprises of data centre and information security services. Previous research indicates that there is no specific framework being develop to mitigate internal threat in the data centre. Findings from the previous study generally show that human resource security, access control, physical and environmental security, and operation and communication security are used to mitigate internal threats. Hence, this paper aims to identify the most important security elements to develop internal threats framework for data centre, as well as to formulate a guideline based on the identified elements. Finally, an internal threats framework based on the elements and the guidelines is developed. A qualitative research technique, such as an interview has been conducted to study the suitability of the identified security control elements. After the result of the first interview, a second interview is conducted to validate the proposed framework. A methodology used to establish the framework includes planning, analysis, design and validation. It is hoped that the establishment of the framework, may guide the public sector to manage internal threats for the data centre, as well as to reduce security incidents which may cause by human factors.

Keywords: *ISMS, ISO27001/27002, internal threat, data centre*

1. INTRODUCTION

ISO/IEC 27001/27002 is widely used in international standard for information security management. The standard consists of a framework used as a guideline for any organization to implement ISMS. The adoption of this standard is to protect critical information, particularly in the public sector. The standard is designed in such a way that it is easy to understand and implemented by the stakeholders. The stakeholder in this term refers to top management, staff, suppliers, customers and regulators [1]. Currently, the ISMS implementation in the public sector mainly focuses on data centre and information security services. The implementation of ISO standard has been recognised in the financial sector due to its requirement to comply with the regulations of the financial. The ISO 27001 and ISO 27002 can be automated easily for policy development and managing risk assessment [2]. Periodical awareness session on the importance of implementing ISMS may reduce security breach faced by organisations. Other benefits of the ISMS implementation are minimizing internal and external security threats and enhance management confidence levels. These benefits can only be achieved if security risks have been identified and managed efficiently. Internal threats such as data sabotage, network sabotage, IT equipment theft, data stolen and e-mail that misused by staff and vendor might be the main source of a security breach in organisations [3]. In order to implement ISMS, we need to consider eleven security controls which are security policy, organizing information security, asset management security, human resource security, physical and environmental security, communication and operation management, access control, information system acquisition, development and maintenance, information security incident management, business continuity management and compliance. The choice of security controls depends on the organization's preference. This preference is based on several criteria such as risk acceptance, risk treatment options, and the general risk management approach. It is also subjected to all relevant national and international legislation and regulations [4]. To design the internal treat security framework, this

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

paper is organised as follows: Section II discusses the research background which is the key issues in this research. Section III explains the related works from past literatures on the research topic. Section IV discusses on the research design and section V explains the analysis and design, while section V concludes the paper.

2. ISMS IMPLEMENTATION

The government agencies normally are aware about the importance of implementing ISMS to ensure information security protection is in placed and adequate in the public sector. The implementation of ISMS in the public sector should be aligned with the government direction. Although, the ISMS standard is continued to be implemented in the public sector, however based on previous research it is found that there is no specific research being conducted in developing a framework specifically focusing on data centre environment to mitigate internal threat. This study focused on the information security control to mitigate internal threat problems in the public sectors' data centres, which may cause by human factors such as the staff and vendors. This study is in accordance with the previous research on the internal threat issue. It is found that most researches on the internal threat issues highlighted human factor as critical elements contributing to the internal threat [5]. Internal threat is the main problem faced by many organizations. Internal threat can be classified as:

- Bad intention of the privileged user, such as sabotage, stealing of intellectual property right, committing fraud and national security crimes by revealing confidential documents;
- Unintentional threat includes negligent use of computing resources [27].

Both internal threat issues such as bad intention of privileged user and unintentional threat relate to any dangerous activities by the staff and vendors is a crucial elements that needs to be emphasized in the framework design. To study on the existing issues of internal treats, reviewing past related documents and journal is conducted. Literature reviews have been conducted involving three main categories of sources, namely (i) data centre policy documents, (ii) academic journals on ISMS and internal threat framework and (iii) documents and academic journals on internal threat. These reviews are deemed necessary in order to understand the current issues on the internal threat and the existing frameworks on ISMS. The findings are reported in the following sections.

2.1 Data Centre Policy

Several data centre policies have been reviewed from existing documents in order to identify important security elements in the policies. Several security elements have been identified in the policies [6] and are reported as follows:

- **Human resource security**
  This element is used in the implementation of Non-Disclosure Agreement (NDA) as the main control for managing staff and vendors.
- **Access control**
  This element is used in the mainframe and database at the access level. Access approval is obtained from various stakeholders through an online system.
- **Physical and environmental security**
  This element is used for managing physical access to data centre using biometric access control. Access approval is obtained from various stakeholders through an online system.
- **Communication and operation management**
  This element is used for managing change management in the data centre in terms of hardware movement as well as software, system configuration and infrastructure changes. Access approval is obtained from various stakeholders through an online system.

It is important to consider the above security elements when designing the internal treat framework.

2.2 ISMS and internal threat framework

Several existing ISMS and internal threat framework have been studied in order to compare the security elements and features that consist in each framework. Five frameworks on ISMS and internal threat have been considered and the findings are reported as follows:

A. ISMS framework

This framework is a general framework for ISMS implementation. This framework used all the eleven security elements exist in the literature. The main element of the framework which relates to internal threat is a risk management element. The framework stated that the implementation of ISMS aims to reduce security threats and vulnerabilities impact in organisations. Small businesses manage

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

their risks as and when needed while big organisations such as banks, telecommunication companies and governments address risk management seriously. Therefore, there is a need to emphasis on the protection of sensitive information or personal data in determination of information security risk [7].

B. ISO Based Security Framework

This framework is a general framework being developed based on ISO 27001/27002 for Information system domain, namely payroll and pensioner system. This framework used all the eleven security elements available in the literature. Plan-Do-Check-Act (PDCA) is the main element in the framework. The phases in the framework are as follows:

- Plan phase – to identify risks through risk assessment.
- Do phase – to implement risk management plan and identify the most appropriate security controls.
- Check phase- to evaluate and establish effective management criteria of the selected corrective action.
- Act phase – to improve and implement the corrective action.

This study briefly mention about internal threats such as user identity impersonation. This internal threats has a high implications and risk, and being classified under the risk of loss and modification of data by the user [8].

C. Integrated Solution for Information Security Framework (I-SOL)

This framework addresses both issues on external and internal threat. I-Sol consists of six components, namely organisation, stakeholder, tools & technology, culture, policy and knowledge. This framework applied three security elements related to the internal threat. These elements are:

- Human resource security as part of stakeholder component.
- Information systems acquisition, development and maintenance as part of tools and technology component.
- Information security incident management as part of the culture component [9].

However, issue in the data centre is not being highlighted in this framework.

D. The Insider Threat Security Architecture Framework (ITSA)

This framework addresses internal threat issues. ITSA has been used as a mechanism to mitigate internal threat caused by authorised users. The main criteria of the framework are as follows:

- Access control enforcement must be in accordance with security control compliance,
- User access control must be in hierarchy such as system owner and user.
- Compliance control by recording audit trails to monitor and control actions [10].

This framework applies two security elements related to the internal threat which is access control elements. This framework also complies with one additional element which is policy. However issues on data centre is not being highlighted.

E. Insider threat Framework

The framework for controlling insider threats to information security is a framework that explains internal threat issues. The framework recommends two methods to enhance security policy effectiveness. These methods are as follows:

- Integrative approach of existing non-IT policy such as corporate and personnel policy with information security policy; and
- Integrative human resources policy such as hiring and termination procedures with security policy to avoid any opportunity for threat. This framework uses access control as the security elements [11].

However there is no issue on the data centre domain being highlighted in this study.

As a conclusion of the reviews on the existing ISMS framework, two common security elements such as human resource security and access control are being used as a component in the framework. The policy and risk have been identified as additional elements to support the implementation of the security controls. Therefore, it is important to include these common elements when designing the ISMS framework.

2.3 Internal Threat Elements

It is important to study other existing internal threat elements that mention in the literature. Several security elements highlighted in the documents and journals and are reported as follows:

Journal of Theoretical and Applied Information Technology
20th December 2014. Vol.70 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- **Human resource security elements**
  This element is required to prevent any misuse of policy, process, procedures or application by insiders [12].
- **Physical and environmental security**
  This element used in biometric system and is required for protection of data and privacy [13].
- **Access control management**
  This element is required to minimize security risk due to attack or threat. Access control in large companies consists of (i) distribution of roles and responsibilities for business users to create and determine level of access (ii) immediate revoke access, in the case of employee dismissal [14].
- **Communication and operation management**
  This element is used in change management for continuous monitoring in managing and identifying the system security level. There are three main elements of continuous monitoring such as IT asset inventory, configuration and change management and managing internal threats due to vulnerability. Configuration and change management include changes to the hardware, system software, communication equipment and all documentation and procedures related to the operation, support and maintenance of the system [15].

As a conclusion from the reviews on the ISMS and internal threat framework, two common elements on security control have been identified, which are: human resource security and access control security. The reviews also identified two other common security control elements with regards to the previous study on data centre policy document. These elements are physical and environmental security. These elements normally used in biometric system and communication, and operation management in change management.

3 RESEARCH DESIGN

In order to propose an ISMS framework, the methodology of this study consists of four phases.

Phase 1: Planning
The activity of this is phase is to understand the problems and issues on internal threat control in the data centre. Four categories of research area were identified and included in this research, which are:

i. Literature review of ICT security policy in public sector.
ii. Literature review of the existing ISMS framework and internal threat.
iii. Literature review on internal threat.
iv. Formulation of interview questions based on the literature reviews. An interview conducted with three respondents, who are the expert in the data centre environment.

Phase 2: Analysis
The activity of this is phase is to analyse ISMS security control elements for mitigating internal threats in the data centre. Further recommendation is made on guidelines for internal threat control based on the selected security elements.

Phase 3: Design
This activity of this phase is to design a conceptual framework for internal threat control based on the selected security elements and recommended guidelines.

Phase 4: Validation
The activity of this phase is to validate the conceptual framework for internal threat control. The validation phase is conducted by interviewing the data centre experts, which are the same experts during planning process.

The research design showed in Figure 1 states the activities and the output in each phase.

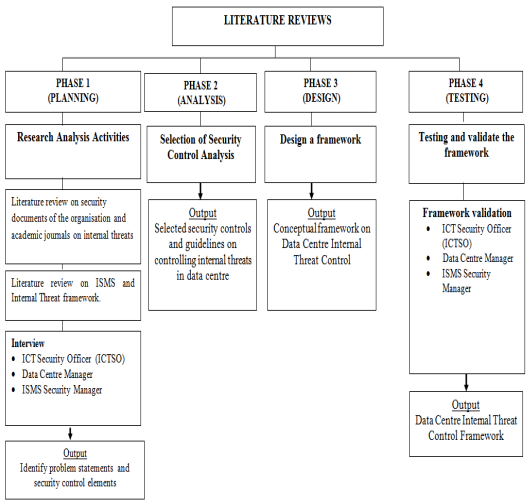

Figure 1. Research Design

3.1 Analysis And Design

Gap analysis has been conducted to analyse the suitability of the security control elements. This

Journal of Theoretical and Applied Information Technology
20th December 2014. Vol.70 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

analysis is conducted by reviewing past research on security control elements [11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26]. The findings are summarized in Table 1. Based on the findings, a list of security control elements and additional elements are identified to support the security elements. The list is as follows:

- Identified security elements:
  - Human Resources Security
  - Physical and Environmental Security
  - Access Control
  - Communications and Operations Management (Change management)
- Selected additional elements:
  - Policy
  - Risk
  - Stakeholder
  - PDCA

Table I: Gap Analysis Interviews

Three categories of literature review to obtain security elements and additional elements to support security controls			Gap analysis interview to identify the suitability of the security elements to mitigate the internal threat
Literature review on ICT security policy in the public sector [6]	Literature review on the existing ISMS framework and internal threat [7, 8, 9, 10, 11]	Literature review on the existing academic journals and documents on internal threat [11, 12,13, 14,15, 16, 17, 18, 19, 20, 21, 22,23, 24,25,26,27]	
Output			
i. Security Control Elements			
a. Human Resources Security b. Physical and Environmental Security c. Access Control d. Communications and Operations Management (Change management)	a. Human Resources Security b. Physical and Environmental Security	a. Human Resources Security b. Physical and Environmental Security c. Access Control d. Communications and Operations Management (Change management)	a. Human Resources Security b. Physical and Environmental Security c. Access Control d. Communications and Operations Management (Change management)
ii. Additional Elements to Support Security Control Elements			
a. Policy	a. Policy b. Risk c. Stakeholder d. PDCA	a. Risk b. Stakeholder	a. Policy b. Risk c. Stakeholder d. PDCA

From this finding it is concluded that the four elements such as human resource security, access control, physical and environmental security and communication and operation management are the most important elements in mitigating internal threats in data centre. Implementation of the security controls needs to be supported by these four security elements such as policy, risk, stakeholder and PDCA.

4. THE PROPOSED FRAMEWORK

The conceptual framework has been developed during the design phase. This framework is designed based on the findings from analysing various academic journals on the internal threat issues. The findings are supported by the gap analysis interview. The interview is to examine the suitability of the selection of the most important security element to overcome internal threats. Subsequently, two frameworks have been selected as a basis to establish a new conceptual framework for mitigating internal threats in the data centre environment, namely ISO based security framework and Integrated solution for information security framework (I-Sol). The conceptual framework is designed based on a combination of these two frameworks. ISO Based Security Framework has been used as a main reference for the basic design of the conceptual framework, while I-Sol serves as a complementary framework. The adoption of the ISO based framework is in line with this research aim which is to develop a framework based on ISO 27001 and ISO 27002. The combination with I-Sol framework is required to complement the conceptual framework in terms of internal threat risk management. The components of PDCA elements in the framework are follows:

- Plan - Identify risk cause by internal threat
- Do- Identify appropriate security controls to mitigate internal threats.
- Check-Select and implement security controls.
- Act-Implementation and monitoring of the security controls based on outline policy and procedures by the stakeholders.

Stakeholder roles and responsibilities are also stated in the framework. The roles and responsibilities are as follows:

- ICT Security Officer (ICTSO) - Responsible in approving non-disclosure agreement sign by staff and vendors to ensure implementation and compliance of the security policies.
- Data Centre Manager and Data Centre Officers – Ensure data centre operation is based on outline security policy and procedures.
- ISMS Manager – Ensure any risk and vulnerabilities is identified and resolved.
- System Administrator – Implement data centre activities based on approval by all stakeholders such as ICTSO, data centre manager and ISMS manager.

Journal of Theoretical and Applied Information Technology
20th December 2014. Vol.70 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

All the components, which are the policy, security elements, the stakeholders' roles and responsibilities, are embedded in the proposed framework. The conceptual framework for mitigating internal threat in data centre is shown in Figure 2.

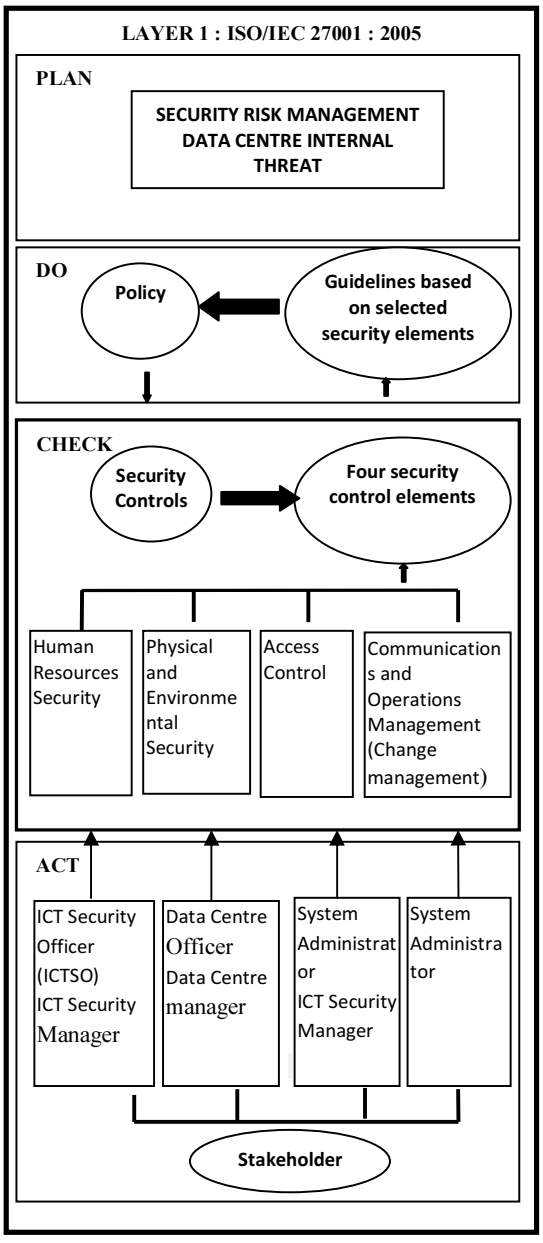

Figure 2. Internal Threat Framework

5 FRAMEWORK VALIDATION

The conceptual framework has been validated via interview by the data centre experts. A further analysis regarding the questionnaire has been derived in order to validate the framework. Five questions are constructed based on the elements of the framework as shown in Table 2. Each question emphasis on the most importance security control elements in order to mitigate internal threat in the data centre. Based on the feedback, all respondents agree with the proposed security elements in the framework as shown in Table 2. Based on the finding from the interview it is confirmed that the framework as proposed in Figure 2 is suitable to mitigate the internal threat for the data centre domain in the public sector.

Table 2: Validation Interview Questions

No	Interview Questions	Feedback by Data Centre Experts
1.	**Element : Security Policy** Does Data Centre security policy depend on the four control?	All respondents agreed that data centre security policy depends on the four control (i) the security of human resources, (ii) physical and environmental security, iii) access control, and (iv) management of operations and communications.
2.	**Element : Security Control Elements** Are security control elements sufficient to overcome internal threats?	All respondents agreed that the selected security control elements, including (i) the security of human resources, (ii) physical and environmental security, (iii) access control, and (iv) management of operations and communications sufficient to overcome internal threats.
3.	**Element : Supporting Security elements** Are additional elements being sufficient to support the implementation of security elements to control internal threats in the data centre?	All respondents agreed that the selected additional elements, including risk management, policy, guidelines and principles of PDCA are sufficient to support the implementation of the security element to control internal threats in the data centre.
4.	**Element : Security Guidelines** Do a comprehensive guideline can be formulated with the four elements of the control?	All respondents agreed that comprehensive guidelines can be formulated with the four elements of the control.
5.	**Conceptual Framework : Internal Threat** Does a comprehensive framework can be established with the adoption of : • Four elements of the security controls, and • Four additional elements to support the implementation of security controls such as risk management, policy, guidelines and principles of PDCA?	All respondents agreed that a comprehensive framework can be developed by adopting : • Four elements of the controls (i) the security of human resources, (ii) physical and environmental security, iii) access control, and (iv) management of operations and communications. • Four additional elements including risk management, policy, guidelines and principles of PDCA.

6 CONCLUSION

The contribution of this study is a framework for mitigating an internal threat for data centre in the public sector based on the ISMS standard. Even though the development of this framework is based on one specific organization in the public sector, it is general enough to be adopted by other government agencies as well. This framework is a generic framework developed based on ISO27001/270002, a standard widely adopted by the public sector. In the future, the internal threats research domain can be expanded to other research domains which include information security services for network security monitoring and management of security incidents in the public sector.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REFERENCES

[1] A. Asosheh, P. Hajinazari, and H. Khodkari, "A practical implementation of ISMS," *7th International Conf. e-Commerce Dev. Countries in Developing Countries with Focus e-Security*, 2013, pp. 1–17.

[2] W. Al-ahmad and B. Mohammad, "Can A Single Security Framework Address Information Security Risks Adequately?," *International Journal of Digital Information and Wireless Communications (IJDIWC)* 2(3), 2012, pp. 222-230.

[3] S. A. Jalil, R. A. Hamid, and A. Aizuddin, "NISER's ISMS Pilot Programme Experiences: Common Shortcomings in ISMS Implementation," 2003, http://www.cybersecurity.my/data/content_files/11/24.pdf.

[4] ISO/IEC 27002:2005(E) International Standard, "ISO 27002 Information technology-Security techniques-Code of practice for information security management," vol. 2005, 2005. http://www.slinfo.una.ac.cr/documentos/EIF402/ISO27001.pdf.(Accessed: 22-Feb-2014).

[5] S. Yang and Y. Wang, "Insider Threat Analysis of Case Based System Dynamics," *Advanced Computing: An International Journal (ACIJ),* vol. 2, no. 2, 2011, pp. 1–17.

[6] Data Centre Policy, *Unpublished Malaysian Public Sector Organisation's Data Centre Policy*, 2013.

[7] A. A. Amarachi and C. Ajaegbu, "Information Security Management System: Emerging Issues and Prospect," *IOSR Journal of Computer Engineering (IOSR-JCE)* Vol.12 (3), 2013, pp. 96–102.

[8] A. Tsohou, S. Kokolakis, C. Lambrinoudakis, and S. Gritzalis, "Unifying ISO Security Standards Practices into a Single Security Framework," in *Proceedings of the South African Information Security Multi-Conference (SAISMC 2010)*, 2010, pp. 188–203.

[9] H. Susanto, M. N. Almunawar, W. P. Syam, Y. C. Tuan, and S. H. Bakry, "I-SolFramework Views on ISO 27001," Asian Transactions on Computers, vol. 01(3), 2011, pp. 1–10.

[10] D. A. Menasc, "The Insider Threat Security Architecture: A framework for an integrated , inseparable , and uninterrupted self-protection mechanism," in *2009 International Conference on Computational Science and Engineering,* 2009, pp. 244–251.

[11] A. Alper, "Controlling Insider Threats With Security Policies," 2011. http://is2.lse.ac.uk/asp/aspecis/20110246.pdf. (Accessed: 8-Feb-2014).

[12] A. Munshi, P. Dell, and H. Armstrong, "Insider Threat Behavior Factors: A comparison of theory with reported incidents," in *45th Hawaii International Conference on System Sciences.* 2012.

[13] S. Ngoma, "Vulnerability of IT Infrastructures: Internal and External Threats," PhD Thesis.2012. http://www.congovision.com/IT-Security-Pub.pdf. (Accessed: 7-Feb-2014)

[14] S. Sinclair and S. W. Smith, "Preventative Directions For Insider Threat Mitigation Via Access Control," pp. 173–202, 2005. http://www.cs.dartmouth.edu/~sws/pubs/ss08a.pdf. (Accessed: 22-Feb-2014).

[15] Computer Network Assurance Corporation(CNA), "Automate Risk Management Framework," 2009. http://www.cnacorporation.com/images/Cyber_Profile_ROI_Paper_3-14-12.pdf. (Accessed: 27-Jan-2014).

[16] H. Susanto and M. N. Almunawar, "Information Security Awareness : A Marketing Tools for Corporate ' s Business Processes," in *Computer Science Journal Advance Access, 2012,* pp. 1–12, 2012.

[17] D. Seo and K. Lee, "Information Security Activities Model per e-Government Service Promotion Stage," in *iiWAS2010, 8-10 November, 2010,* pp. 8–10.

[18] G. Silowash and T. J. Shimeall, "Common Sense Guide to Mitigating Insider Threats 4 th Edition," *Technical Report CMU/SEI-2012-TR-012 CERT® Program*.2012. http://resources.sei.cmu.edu/asset_files/TechnicalReport/2012_005_001_34033.pdf. (Accessed: 8-Feb-2014)

[19] M. E. Whitman, "In Defense of the Realm: Understanding the Threats to Information Security," in *the International Journal of Information Management*, vol. 24, 2004, pp. 43–57.

[20] F. L. Greitzer, D. Ph, and R. E. Hohimer, "Modeling Human Behavior to Anticipate Insider Attacks," *Journal of Strategic Security Volume 4 Number 2 Summer 2011: Strategic Security int the Cyber Age,* 2011, pp. 25–48,.

[21] A. B. M. Z. Z. P. Nelson, "Security Threats Of Computerized Banking Systems (CBS): The Managers' Perception In Malaysia," *International Journal of Economics And Finance Studies Vol 4, No 1, 2012* pp. 21–30.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[22] S. Pramanik, V. Sankaranarayanan, S. Upadhyaya, and B. Hall, "Security Policies to Mitigate Insider Threat in the Document Control Domain," in *Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC'04)*, 2004.

[23] A. Klaic, "Overview of the State and Trends in the Contemporary Information Security Policy and Information Security Management Methodologies," in *MIPRO 2010, May 24-28, 2010,* pp. 1203–1208.

[24] I. Shield, "The Insider Threat-Security Policies to Reduce Risk," *Information Shield Whitepaper*, pp. 1–9, 2010. http://www.informationshield.com/papers/Security%20Policies%20Address%20the%20Insider%20Threat.pdf.[Accessed: 22-Feb-2014].

[25] T. R. Cappelli, Dawn, Moore Andrew, "The Cert Guide to Insider Threats," SEI Series. A Cert Book, 2012. http://ptgmedia.pearsoncmg.com/images/9780321812575/samplepages/0321812573.pdf. (Accessed: 27-Apr-2014)..

[26] S. Gupta and A. K. Saini, "A Review to Assess Insider Threats and Management of Security Risk in An Organization," *International Journal of Trends in Computer Science Volume 2, Issue 11, 2013, pp:7462 – 8452*.

[27] T. E. Senator, E. Chow, "Detecting Insider Threats in a Real Corporate Database of Computer Usage Activity," *Proceeding The 19th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining - KDD '13*, p. 1393, 2013.