ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 3, pp: (64-67), Month: July - September 2014, Available at: www.researchpublish.com

Collation B2B e-line System Security Threats

[1]Rahul, [2]Ms. Sunita

[1]M.Tech. Student, Shri Baba Mastnath Engineering College (SBMEC)
Maharashi Dayanand University (MDU), Rohtak
[2](HOD of Computer Science Department in Shri Baba Mastnath Engineering College) (SBMEC)
Maharashi Dayanand University (MDU), Rohtak

***Abstract*: The chapter range was AN introduction to the BS 7799 that's utilized in analysing the safety threads of the system. during this chapter, we have a tendency to go deeper to the BS 7799 procedure and undergo every step of the ISMS method. As what it involves this thesis work this chapter is additional theoretical than analytical and does not have direct contact to the BS 7799 auditing method.**

***Keywords:* B2B e-line system, security threats.**

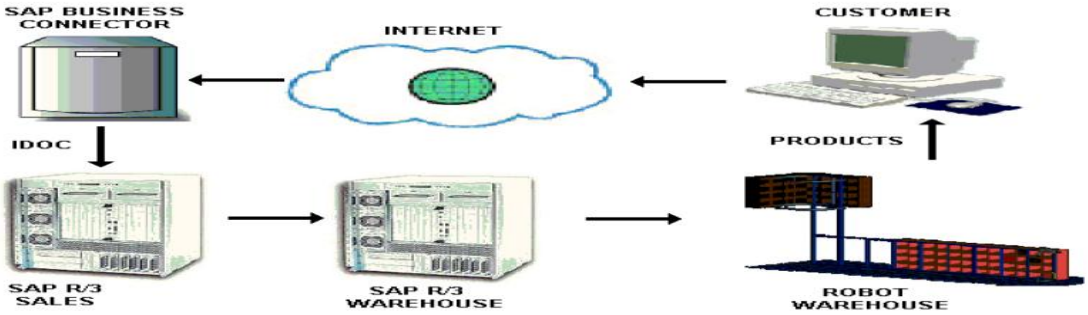
I. INTRODUCTION

The history of BS 7799 starts on the year 1987 when United Kingdom's Department of Trade and business (DTI) based business laptop Security Centre (CCSC). CCSC's task was to define a group of rules that would be used to value IT companies' security levels. The set of rules would conjointly act as a suggestion to the businesses attempting to determine secure ways that of constructing business. One goal was conjointly to induce the made customary international recognized. [1] 7799-1 was free within the year 1995. within the year 1998 BS 7799-2 was released as a further half to BS 7799. recreate of BS 7799-1 was released within the year 1999. BS 7799-1:1999 became internationally recognized in the year 2000 once world organisation of standardization (ISO) accepted it by name ISO/IEC 17799:2000. Second a part of BS 7799 got conjointly revision within the year 2002, however it's not nevertheless internationally recognized. [1]

E-Line:

The idea for e-line surfaced once the quantity of orders returning from subsidiaries and agencies began to grow speedily. the most production sites and offices in Germany introduced SAP management programs to their operate within the 90's thus e-order system became doable to implement with cheap quantity of work and resources. SAP R/3 atmosphere was appropriate process orders and it combined to state of the art automaton warehouse looked terribly fascinating environment for e-order framework.

The other reason why e-orders were found terribly appropriate commutation the regular orders were the sort of merchandise handled. Most of the massive customers recognize exactly what they need even months before the particular delivery time. Processing these forms of orders with e-order system will be automatic simply.



Exploitation the BS 7799 to enhance organizations information security:

The chapter range was AN introduction to the BS 7799 that's utilized in analysing the safety threads of the system during this chapter, we have a tendency to go deeper to the BS 7799 procedure and undergo every step of the ISMS method. As what it involves this thesis work this chapter is additional theoretical than analytical and does not have direct contact to the BS 7799 auditing method.

The main reason for this chapter is to provide AN unified image of info the knowledge the data security processes and gift a model that might facilitate organization to attain level of data security outlined within the BS 7799.

Totally different sub stages of the ISMS designing part:

There area unit six totally different steps on ISMS designing part. These totally different phases and their sequence will be found from the Figure two. within the chapter , there was a brief intro to all or any of those steps and the way they're outlined in BS 7799-2. In this chapter all of those six chapters area unit competent additional accurately and there the purpose of read isn't solely chosen from the quality however from alternative sources and from the own experiences conjointly. [2]

Outline the policy:

A statement of management's intent. This part's purpose is to support the goals and principles of the data security policy. The half wants to offer a transparent image why this document is very important and why it ought to be well understood by each member of the employees. [2, 4]

II. THE SCOPE

The scope defines what the target of ISMS is typically the scope will be outlined to be the complete organization, however typically it's additional beneficiary to target some more space. once the target of ISMS is outlined, it's necessary to choose the area unit as that are centered on. These areas may for instance be databases, information, personnel, facilities, applications hardware and software or communications hardware and software system. the dimensions of the target is one of the most factors that outline however mere information ISMS produces

A risk assessment:

The operate of the chance assessment is to find all the risks that have a notable result to the organization. the primary step of this method is to search out all the risks that organization faces. The second step is to search out out what risks area unit actual ones. [2, 5]

Choose management objectives and controls:

Selecting controls and objectives that area unit controlled may be a field that BS 7799 will not provide an easy resolution. the primary step to choosing controls has been done when security necessities are chosen. The risks that are defined within the risk assessment want typically controls. These controls will facilitate reduce the risks to the suitable level. This acceptable level of risks ought to be defined within the scope of ISMS. [2]

Manage The Risk:

Choosing the acceptable approach to risks that area unit outlined applicable risks in risk assessment section is typically terribly troublesome. In Figure six there's a flowchart that presents the trail of the threat to the particular risk. There area unit four properties that require to be consummated. Eliminating any of those four properties can neutralize the chance. One approach may well be hunting this flow sheet and make the choice on that stage the chance is eliminated supported the 'least- cost'- principle. typically over one threat will be neutral with one countermeasure. If over one risk is eliminated it's to be taken underneath evaluation once hard the value of risk neutralization. [3, 6]

Doing an enclosed auditing method

An internal audit is that the one the foremost necessary tools once making an attempt to enhance to information security level of the organization. With internal audits, the actual level of the organizations data level is measured. additionally once making an attempt to accomplish official certificate, before the skin evaluators area unit invited to the organization, internal auditing processes ought to be wont to discover as several weaknesses and defiencies as potential. This chapter tries to explain associate effective thanks to do an enclosed audit considering the strain found from BS 7799-2. [3, 4, 7]

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 3, pp: (64-67), Month: July - September 2014, Available at: www.researchpublish.com

Totally different stages of the audit procedure

Before audit method is started the scope of the audit needs to be chosen. The scope of associate audit will vary from everything of checking one service or control to the complete BS 7799-2 audit procedure. the sole official demand set in BS 7799-2 is that ISMS method is audited once a year. [3]

The planning stage is that the start of the inner audit. when the scope and objective are chosen auditing methodology needs to be set. There are several alternative ways to execute auditing method and every of them has their advantages and downsides. once selecting methodology to use, price potency has to be taken into account. totally different potential ways are: expedited meetings, Interviewing, Questioning, Observation and review, Documentation Review, confirmation/ Representation, review, Data Analysis, Vouching & validatory, method mapping, method tracing, Surveys, Scanning, Reconciliation and calculation & Valuation. additional regarding these methods is scan from Appendix C. once methodology is chosen arrangement can be created. These arrangements embrace assignment resource and time for the both parties of the audition, auditor and auditee and informing necessary stakeholders regarding the auditing event. [7]

The ways employed in this audition were principally Interviewing, Questioning, Document Review and Observation/ Inspection. the explanation why these ways were chosen was that the goal of the audit was offer overall mage of the information security level within the organization. the opposite goal was to search out out as several defiencies as potential and these ways area unit smart during this.

The next step is actual auditing. throughout the auditing procedure, special effort has to tend to identify the actions and tasks that don't seem to be within the satisfactory level. additionally detection the foremost vital fields that require improvement is crucial. Results of the auditing method have to be compelled to be recorded properly that they'll be used effectively in later stages. [7]

The actual auditing method was conducted throughout Gregorian calendar month 2004. It took approximately forty hours of labor together with the preliminary actions done on the site. After auditing is finished, succeeding logical part is reviewing the work. During the reviewing part conclusions and complete performance of the auditing set up is confirmed. coverage has to be done to the management that's accountable of the sector audited and to the data security management.

III. OBJECTIVES

An internal audit has 2 main objectives that it has to fulfil. the primary one is to confirm that the correct individuals have performed the procedures that area unit outlined in ISMS or in alternative necessary documents. The second objective is to substantiate the results that the ISMS activity produces area unit the correct ones. In Table , there are some samples of what may well be the particular objectives of an enclosed audit. [3, 4, 7]

Objective	Sample task
Confirm the processes	• The access rights to the system are approved by person how is named responsible of access right management. • The risk management procedures are followed and there can be found written risk assessment documentation.
Confirm the results	• Verify that the access right given to somebody are appropriate for the task he/she is doing. • Verify that all the risks were identified in risk analysis phase of ISMS.

IV. RESULTS

The result section holds the data received from the audit method exhausted the organization. The audition of the organization was finished 3 totally different methods. The ways were work the work space, work practices and conducting a series of interviews with totally different individuals from the organization.

1. Security policy
2. Security organization
3. Asset classification and control
4. Personnel security
5. Physical and environmental security
6. Communications and operations management

REFERENCES

[1] Dr. David F. C. Brewer, ISO 17799 Summary , Gamma Secure Systems Limited, 2004, White Paper, Available at: http://www.gammassl.co.uk/bs7799/, Reference June 04 , 2014

[2] Anonymous (Committee BDD/2), Information security management, BS 77991:1998 Code of practice for Information security management, 1998, British standards.

[3] Anonymous (Committee BDD/2), Information security management, BS 7799-2:1999 Specification for Information security management systems, 1999, British standards

[4] William List, Doing an internal audit, ISMS Journal issue 3 (Angelika Plate), ISMS International User Group Ltd, April 2004, Journal

[5] Anonymous (University of Florida Computer science division), Information Technology Security Policy. University of Florida, UF Office of Information Technology, 2003, Web publication, Available at: http://www.it.ufl.edu/ policies/ security, Referenced June 28 , 2004

[6] Gary Stone burner, Alice Goguen, and Alexis Feringa, Risk Management Guide for Information Technology Systems - Recommendations of the National Institute of Standards and Technology, the National Institute of Standards and Technology, 2002, NIST special publications, Available at: http://csrc.nist.gov /publications /nistpubs/, Referenced 8, 2004

[7] Anonymous, Internal audit tools and resources, Protiviti Inc. EOE. 2004, web publication, Available at: http://www.knowledgeleader.com, Referenced July 12, 2004