#48 RISK ASSESSMENT, IMPACT ANALYSIS AND CONTROL METHODOLOGY VIA DIGITAL DASHBOARDS IN STATISTICS DATA CENTERS

Mr. Atif Amin, Dubai Statistics Center, Dubai, United Arab Emirates, atif_amn@hotmail.com
Dr. Raul Valverde, John Molson School of Business, Concordia University, Montreal, raul.valverde@concordia.ca.
Dr. Malleswara Talla, Department of MIE, Ryerson University, Toronto, mtalla@ryerson.ca

ABSTRACT

Every system, when connected to a network, is susceptible to threat of being hacked. It is important to protect all systems of an organization in real-time in a cost-effective manner. This paper presents a well-designed and integrated database for risk management data using a dashboard interface in real-time risk that makes it easy for risk managers to reach a understanding the level of threats to be able to apply right controls to mitigate them. In this paper, a case study of a data center for a statistical management institute is presented that proposed calculation of total risk at the organization level by using the proposed risk database. A digital dashboard is also designed for presenting the risk level results so that decision makers can apply counter measures. The risk level on a dashboard viewer makes it easy for decision maker to understand the overall risk level at the statistics data center and assists in the creation of a tool to follow-up risk management since the time a threat hits till the time of its mitigation.

Key words: Dashboard, Watchdog system, Risk database, Risk management expert system, Data center.

INTRODUCTION

A data center is a complex facility with several computer systems, telecom equipment and storage systems. The data centers have been successfully implemented in commercial sectors. The data centers for statistics purposes has been growing rapidly in the financial market and health care (Khan & Valverde 2013). Dashboards for risk visualization have been suggested in the past, Eppler & Aeschimann (2009) suggested a dashboard for risk communications but did not address the issue of risk factors calculations, other authors have suggested dashboard for enterprise risk management but not specifically for the use of calculation of risk factors in data centers (Scarlat, Chirita & Bradea 2012).The research focuses on conceptual understanding of information technology assets, how assets can be classified and presented in a risk database, primary focusing on designing and building a successful Information Security Management System (ISMS) module that can help statistics data for early detection of business risk. The following steps illustrate the scope of the research work:

1. Categorize assets into tangible assets (hardware, software) and intangible (data, Services and company Image)
2. Classify assets (assign access to applications and documents to various levels of management).
3. Group assets in types as (Hardware, Software, Data, Files, Services, Hard Documents… etc)
4. Identify organization’s main services and related business processes
5. Build a relationship between assets and business and store information in a relational database.
6. Identify threats, vulnerabilities and possible impacts through risk assessments, history records, and literature.
7. Create an automated Risk Assessment Plan (RAP) that allows the easy retrieval of risk information.
8. A business continuity plan based on assets and risk treatment plan (RAP) and a risk mitigation plan.
9. ITIL based Asset Management Database (CMDB) for enhancing and maintaining Information security in statistics data centers.

The results should lead to investigating risk causes using a dashboard viewer that will help IT managers to analyze results and establish proper controls to mitigate risk in statistics data centers.

THEORETICAL BACKGROUND ON RISK MANAGEMENT

The study focuses on understanding risk components and their related threats over statistics data centers assets; in particular the study is going to explore in more detail the risk’s causes and reasons and will attempt to find solutions and controls to protect businesses. The paper reviews the following: Assets, Threats and Vulnerabilities, Impact, Risk management, Risk Assessment, and Risk Mitigation. Risk management consists of three major processes (Landoll 2006): Risk Assessment, Risk Mitigation, Risk evaluation and Assessment. Residual Risk can be defined as the value of risk remaining after risk mitigation (Kouns & Minoli 2010). The Term Residual Risk is used as the acceptable level of threat that organization can bear and survives with. To distinguish Residual Risk from Total Risk, Harris (2008) clarifies it in the Equation 1, which is:

$$\boxed{\text{threats} \times \text{vulnerability} \times \text{asset value} = \text{total risk}}$$

(threats × vulnerability × asset value) × controls gap = residual risk

Harris (2008) also illustrates Residual Risk in Equation 2, which is:

(threats, vulnerability, and asset value) = total risk
total risk – countermeasures = residual risk

Organizations must work out a way of evaluating the total and residual risks to mitigate.

Asset's Attributes for Risk Database

Assets types can be: Information Assets (electronic files, data), Paper copy documents (contracts, manuals, plans, agreements, correspondences), Software assets (systems, applications), Physical assets (Computers, Storages, Network devices, Cables, Power devices), and People (Technical staff, Customers and Clients). Asset management includes knowing and keeping up-to-date this complete inventory of hardware (systems and networks) and software (Harris 2008). To keep track of assets, Configuration Management Database (CMDB) and Assets inventory should be synchronized to keep track of changes and incidents and vulnerabilities (Harris 2008). A well-defined asset lifecycle process starts from acquiring the asset till write-off. Based on ISO27001 best practices information assets are to be well identified at risk assessment.

METHODOLOGY

Design-science research methodology is chosen as a framework for the study given the applied nature of the research. This methodology has a history of providing good results in the evaluation of constructs and models in information systems (Peffers et al. 2007) (Valverde et al. 2011). Design science in information systems is defined by March and Smith (1995) as an attempt to create things that serve human purposes, as opposed to natural and social sciences, which try to understand reality. March and Smith (1995) identify build and evaluate as the two main research activities in design science. Build refers to the construction of constructs, models, methods and artifacts demonstrating that they can be constructed. The research in this paper is based on the design science framework detailed above and essentially covers the ***build*** and some ***evaluate*** research activities and has a research output of ***constructs*** and ***models***. The build part of this research was implemented with the data model for the risk management database. The ***Instantiation*** component of the research was implemented by implementing a database artifact based on the proposed risk management data model. The evaluate part of the research was implemented with a risk management dashboard for a selected case study used to evaluate the database model proposed for the risk management of data centers.

The risk management methodology follows a case study that investigates primarily a situation, problem, company, or group of companies (Dawson 2009). Secondary data was collected from related books, journals, on-line articles, vendors' websites and technology news websites. The case study used for this research is the statistics data center of Dubai. The design of this study is based on well-known risk management methodologies are: (1) National Institute of Standards and Technology (NIST) in their Risk Management Guide for Information Technology System describes a full Risk Management Cycle; NIST Framework based on three processes; Risk Assessment, Risk Mitigation, and Evaluation and Assessment, (2) IT Governance: A manager's Guide to Data Security and ISO 27001/ISO 27002 based on well-defined activities that can be modified to fit any organization's Information Security Management System (ISMS) needs, based on Gap Analysis, identifying criticality, potential threats and vulnerabilities, Risk Treatment Plan and the selection of controls and statement of applicability, Measures of Effectiveness. The figure 1 illustrates the best practices, risk assessment processes following NIST 800-30.

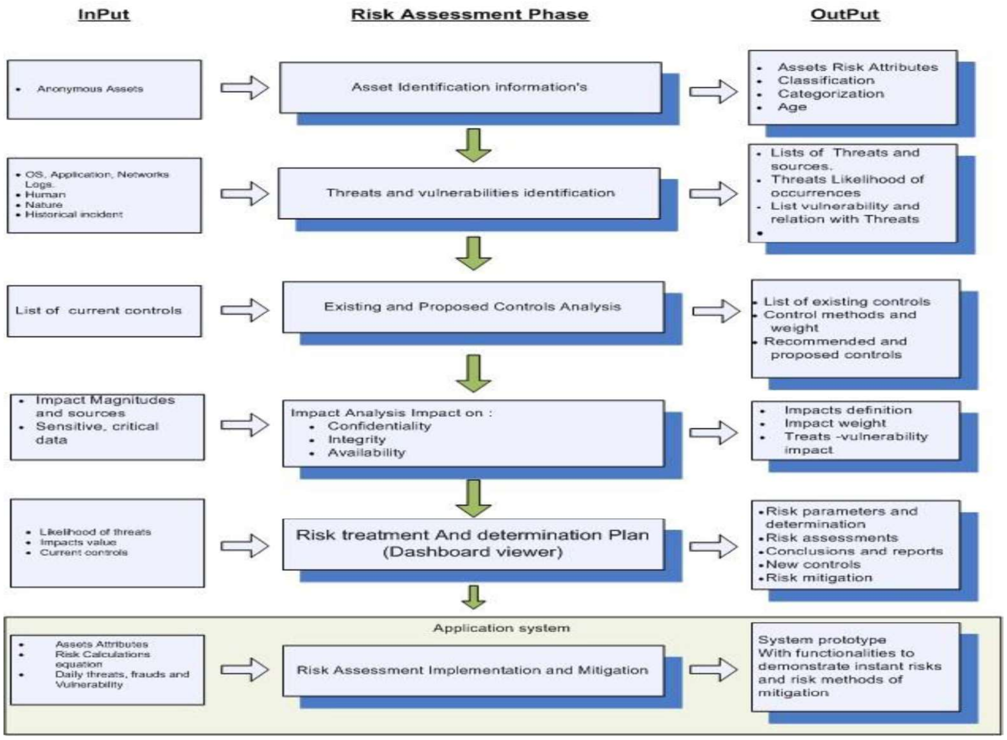
InPut
Risk Assessment Phase
OutPut
Anonymous Assets
Asset Identification information's
Assets Risk Attributes
Classification
Categorization
Age
OS, Application, Networks Logs.
Human
Nature
Historical incident
Threats and vulnerabilities identification
Lists of Threats and sources.
Threats Likelihood of occurrences
List vulnerability and relation with Threats
List of current controls
Existing and Proposed Controls Analysis
List of existing controls
Control methods and weight
Recommended and proposed controls
Impact Magnitudes and sources
Sensitive, critical data
Impact Analysis Impact on :
Confidentiality
Integrity
Availability
Impacts definition
Impact weight
Treats -vulnerability impact
Likelihood of threats
Impacts value
Current controls
Risk treatment And determination Plan (Dashboard viewer)
Risk parameters and determination
Risk assessments
Conclusions and reports
New controls
Risk mitigation
Application system
Assets Attributes
Risk Calculations equation
Daily threats, frauds and Vulnerability
Risk Assessment Implementation and Mitigation
System prototype With functionalities to demonstrate instant risks and risk methods of mitigation

Fig. 1 Risk Assessment phases based on NIST SP 800-30

Information Information Gathering Methods and Tools

The process emphasizes on carrying a sequence of interviews with asset's owners, stakeholders, technical teams and risk related organization's members (Landoll 2006). The stakeholders can be: the assets owners, technical administrators, information security specialists, business owners, risk manager, finance manager, and top managers. Interviews to key personnel help to determine their ability to perform their duties, and observations or concerns (Landoll 2006). Questionnaire is just a passive version of an interview (Wheeler 2011). The development of a set of interview questions depends heavily on the security risk assessment method, scope, and budget being applied (Landoll 2006). All surveys and questionnaires are designed based on Dubai Statistic Center working environment and based on best practices of: Calder and Watkins (2008) and Stoneburner et al. (2002). Proposed templates, questionnaires and interviews with stakeholders and technical team are to be completed and approved by top management. The templates can be: (1) collecting assets information via Assets Classification and Categorization Template, and Assets details from Inventory System, (2) Collecting threats and vulnerabilities Information using "General Threats Identification Sheet", (3) Collecting existing controls using: "Controls" template, (4) Collecting Impact Analysis details using: Qualitative Risk Assessment Template, and Quantitative risk assessment template.

Qualitative risk assessment methodology

The Statistics Center of Dubai conducted value based evaluation by categorizing the assets into high, medium, and low value. The parameters considered are: the asset dependency level (how important it is), asset access level (how often referred to), and asset age. Besides assets' data threats information must be well identified and collected to correctly weight their impact values. Threats must be identified, classified by category, and evaluated to calculate their damage potential to the company (Harris 2008). Based on best practices at Dubai Statistic Center threats data can be gathered from: Historical systems attacks, World wide data, Surveys and Questionnaires. Threat's historical data can be a good reference to organization's Information Security procedures. Threat probability of occurrence can never be 100% accurate after all it is not easy to predict when the next attack will be, however, giving a weight to threat's likelihood of occurrence can lead to better determination of risk value. The likelihood that a potential vulnerability could be exercised by a given threat-source can be described as high, medium, or low (Stoneburner et al. 2002). Referencing NIST SP 800-30 (Stoneburner et al. 2002) and based on the Dubai Statistic Center, business sensitivity in the following table illustrates impact volume measurement:

Table 1: Impact volume Measurements based on NIST SP 800-30

Impact Volume	Description
Insignificant	Almost no impact if threat and vulnerabilities are exploited
Minor	Minor effects on organization's assets and business, recovering is manageable
Significant	Results in some tangible damage, and require some time to recover (example internal service interruption and restored, connection down restored immediately)
Damaging	Noticeable impact that result in large but internal damage, requires time and resources to restore (example internal operation failure)
Critical	The impact could result in high damage of business infrastructure which result total failure to deliver business and require long time and high resources to restore (example production server failure, network down)

The approach assigns a weight to each asset, threat's impacts and their likelihood of occurrences as (High, Medium and Low). Risk is calculated in the proposed risk database as defined in Equation 3 (Harris 2008):

Risk =Asset Value X Impact X Likelihood of Threat

Quantitative risk assessment methodology

To evaluate monetary risk, the assets are measured in currency in terms of tangible financial costs such as Market Cost, Development Cost in case of software, Installation and Configuration cost, Maintenance and Support Cost, Replacement Cost, Operation and running Cost (electricity, License in case of software), and Depreciation Cost. The asset value is derived using the equation 4, as follows:

Asset Value = Purchasing Value - Depreciation value + (cost of time to recover) or cost to replace asset and put it to functioning + loss caused by service stopping+ Support and Maintenance value

The exposure factor (EF) represents the percentage of loss a realized threat could have on a certain asset (Harris 2008), (Kouns & Minoli 2010). Single Loss Expectancy (SLE) is the total amount of revenue that is lost from a single occurrence of the risk (Kouns & Minoli 2010). Annual Rate of Occurrence (ARO) is the normalized rate at which the risk exposure resulting in actual damage occurred for one year (Kouns & Minoli 2010). The annualized rate of occurrence (ARO) is the value that represents the estimated frequency of a specific threat taking place within a one-year timeframe (Harris 2008). Qualitative risk is based on assigning monetary value to assets. Based on Harris (2008), Tan (2002) and Wheeler (2011) the quantitative risk formula in the proposed risk database is calculated in equation 5, as below:

Single Loss Expectancy (SLE)= Asset Value *Exposure Factor (EF)
Annual Loss Expectancy (ALE) =SLE X Annual Rate of Occurrence (ARO)

RISK MANAGEMENT ARCHITECTURE IN THE CASE STUDY

The network and systems architecture of Dubai Statistics Center is presented in figure 2, that enables users to identify vulnerabilities.

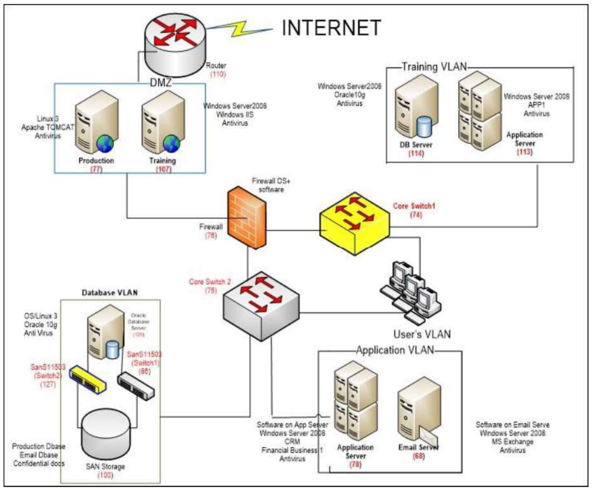

Fig. 2 IT service infrastructures

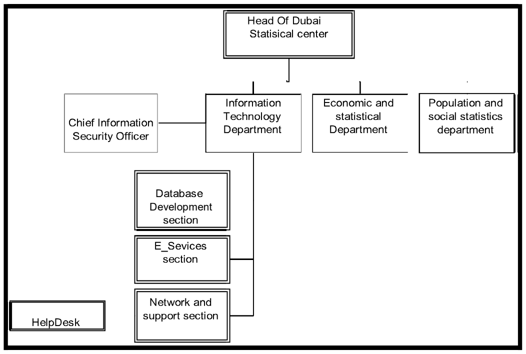

Fig. 3 Dubai Statistic Center Organization Chart

The risk team can plan risk management processes, contacts in case of failure, the impacted departments in case of a threat and possible loss. Figure 3 represents part of the Dubai Statistic Center's Departments Organization Chart.

Assets Information Identification

The first step is to collect assets' data based on importance regarding assets' type, nature, mean of storage, owner and access privilege. The second step is to collect assets' info based on its logistic storage where assets' details are to be recorded. The collected data can be pushed later to a risk database. Based on a template and the Dubai Statistic Center Infrastructure in figure 2, the data collected was based on: Storage media, Physical Location, Owner, Acceptable Use etc. The required risk data are collected and coded using the proposed excel sheets as to be used later to feed the risk database as the schema is presented in Figure 5.

Collecting Controls and Quantitative Risk Data

Based on best practices and interviews conducted with related members and business owners, the following a proposed template in figure 6 is used to gather existing controls applied to certain assets. Based on the risk formula and previous data collected via assets, threats and controls templates, risk values were derived against assets before and after the proposed controls. Based on risk formula and previous data collected via assets, values, threats and expected loss factors, risk values in figure 8 illustrates the calculation of risk values against asset before and after proposed control. The following figure presents electronic threats sources to risk database.

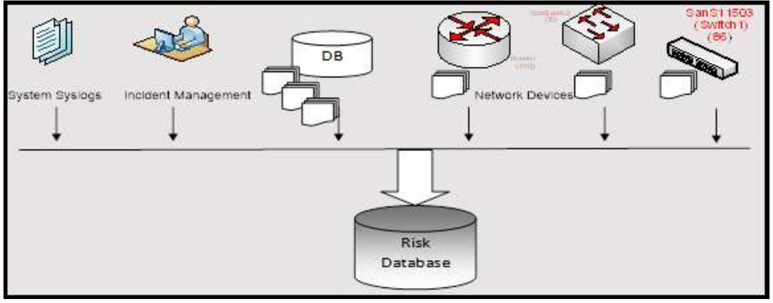

Fig. 4 sources of threats

Design and build risk database

The database design includes entities that define risk processes, attributes which constructs each entity and relationship between entities. Based on a template, the details of Assets, Threats, and Controls are collected, and the entities are broken down into sub-entities based on collected data. The data collection is based on surveys and questionnaires provided and it is more achievable when it comes to rate similar hardware that exists in two different businesses (example a Server can be rated as HIGH when it comes to production environment while the same Server can be rated as LOW if it is used for training purposes). A monetary value presentation of assets, threats and risk, for those who seeks financial numbers can use the Quantitative values which is part of the risk database.

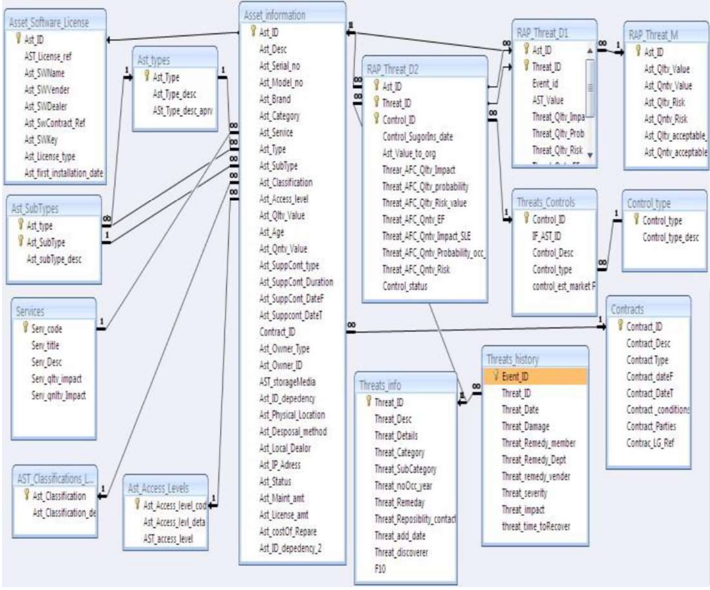

Fig. 5 database design

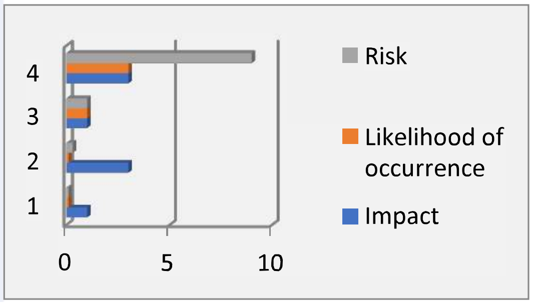

Fig. 6 Dashboard View: High-Risk based on threat's impacts

DIGITAL DASHBOARD COMPONENTS AND RISK ANALYSIS

A dashboard viewer can provide various risk info that can help the risk team to determine what action needs to be taken. Actions should be based on decisions that's wisely reflects the risk volume and amount of damage that can result. Three risk scenarios are presented to demonstrate the risk dashboard generation for risk management.

Risk scenario 1: Threats and Impact Analysis based on Qualitative approach

Data at the proposed dashboard viewer can be presented as Charts and Tables. The risk manager in this case is looking for assets or systems with high impact value and low likelihood of occurrence or high impact value and high likelihood of occurrence. The results are presented in the dashboard view in figure 6.

Risk scenario 2: Decisions based on Historical Risk Data

Risk historical data can be a reliable source for decision makers and risk analysts for the planning of risk mitigation strategies. The risk database through dashboard views can help to make a better picture of the nature and types of threats for frequent attacks and their business impact. Based on the analysis of the dashboard, an analyst can decide if an action needs to be taken towards this risk and to whether add more controls and propose prevention actions or just accept the risk. Based on the historical table in Risk Database the (qualitative and quantitative view) risk values can shows increases of risk through years as seen in figure 12. Retrieved data filtered by threat number 25 (Unauthorized access), shows that this threat's impact is increasing over the years (2009, 2010, 2011) as indicated in the dashboard view in figure 13. Figure 14 shows a dashboard view that indicates IBM SAN Storage, MS Exchange Server and Oracle Database server are subject to "Unauthorized Access". This threat is increasing every year.

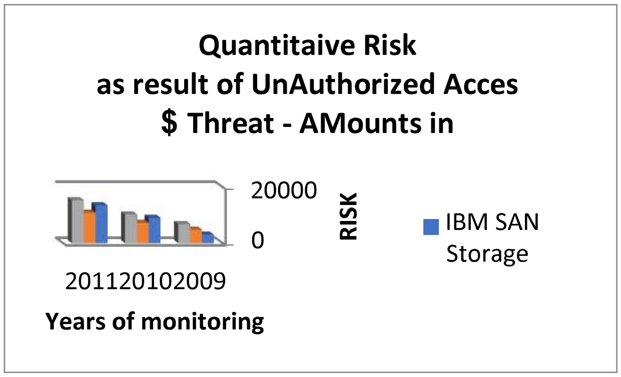

Fig. 7 Dashboard: Annual increases of Asset's risk- chart view

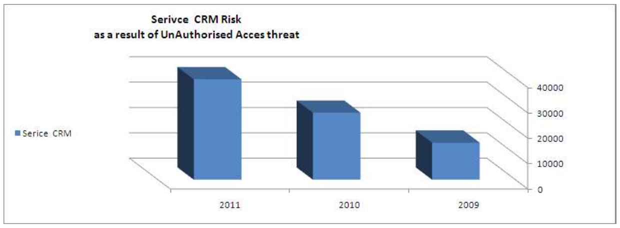

Fig. 8 Dashboard: Annual unauthorized access risk of service level

Risk scenario 3: Risk views at CRM service level

The Risk database can provide risk views at the service level (example CRM) where all related assets risk values are added as a sum as shown in figure 15. Based on previous analysis and investigation to "unauthorized access", a new control is proposed and the next figure illustrates the risk level after the new control is applied (Purchasing IPS

The above figure and based on quantitative risk analysis shows drop in risk level to 1000$, 2400$ and 3400$ to IBM SAN Storage, Email Server and Oracle Server respectfully at 2011 and after new control is applied.

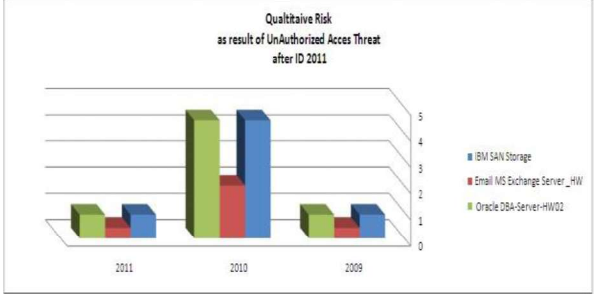

Fig. 9 Dashboard: Qualitative-risk dropped in 2011 to acceptable level

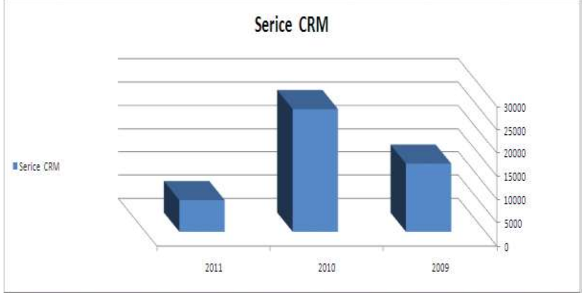

Fig. 10 Dashboard: Service level risk acceptable in 2011

The above figure and based on qualitative risk analysis shows drop in risk level to 0.9, 0.4 and 0.9 to IBM SAN Storage, Email Server and Oracle Server respectfully at 2011 and after new control is applied.

As a result, CRM service Level risk is dropped to reach level less than what was in 2009 as shown in Figure 18.

CONCLUSIONS

The calculation of total risk at a statistics data center based on qualitative and quantitative analysis is possible using the proposed database that will give decision makers a good insight to make better decisions before and when threats hit the organization. Predicting threats before they happen by conducting a what if analysis on the infrastructure and calculate the expected risk, take the propriety action as preventing threat from happening or mitigate risk before it happens is possible with a help of a dashboard in a statistics data center. Presenting the risk level on a dashboard viewer makes risk level clearer for a decision maker. The model created with the help of managers, head section, risk officers, helpdesk (risk stakeholder) of a statistics data center assisted in the creation of a tool to follow-up risk management since the time it hits till the time of mitigation, and it will give a clear picture for a manager on how subordinates are performing. Historical risk data is a good and rich source to threats and impacts that surrounds the statistics data center organization. Decisions can be built based on legacy information to provide better protection and controls can minimize manual activities and paper work. The main contribution of the paper is a design of a risk management database in order to support the decision support for risk managers for data centers. The main lesson learned is that databases have potential for risk management support in data centers. Future research can be focused on the design of a standard data model that can be used for all the data centers for risk management purposes.

REFERENCES

Almadhoob, A, Valverde R.: Cybercrime Prevention in The Kingdom of Bahrain via IT Security Audit Plans. Journal of Theoretical and Applied Information Technology 65, no. 1, p.p. 274-292 (2014).

Calder, Alan, Steve Watkins, and I. T. Governance. "A Manager's Guide to Data Security and ISO 27001/ISO 27002." Kogan Page (2008).

Dawson, C. W. Projects in computing and information systems: a student's guide. Pearson Education, (2009).

Eppler, M. J., & Aeschimann, M. (2009). A systematic framework for risk visualization in risk management and communication. Risk Management, 11(2), 67-89.

Harris, Shon. CISSP all-in-one exam guide. McGraw-Hill, Inc., (2008).

Khan, N. A., and Valverde R.. "The use of RFID based supply chain systems in data centers for the improvement of the performance of financial institutions." Engineering Management Research 3, no. 1, pp. :1-24 (2014).

Koons, J., Minoli D.. "Information Technology Risk Management in Entreprise Environments.", John Wiley and Sons Inc (2010)..

Landoll, D.. The security risk assessment handbook: A complete guide for performing security risk assessments. CRC Press, (2006).

March, S. & Smith, G. 1995, 'Design and Natural Science Research on InformationTechnology', Decision Support Systems, vol.15, no.4, pp. 251 - 266.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of management information systems, 24(3), 45-77

Scarlat, E., Chirita, N., & Bradea, I. A. (2012). Indicators and metrics used in the enterprise risk management (ERM). Economic Computation and Economic Cybernetics Studies and Research Journal, 4(46), 5-18.

Stoneburner, Gary, Alice Y. Goguen, and Alexis Feringa. "Sp 800-30. risk management guide for information technology systems.", National Institute of Standards and Technology (2002).

Valverde, R., Toleman, M., & Cater-Steel, A. (2011). A method for comparing traditional and component-based models in information systems re-engineering. Information Systems and e-Business Management, 9(1), 89-107.

Wheeler, Evan. Security risk management: Building an information security risk management program from the Ground Up. Elsevier, (2011).