Metadata of the chapter that will be visualized online

Chapter Title	Using Dashboards to Reach Acceptable Risk in Statistics Data Centers Through Risk Assessment and Impact Analysis	
Copyright Year	2017	
Copyright Holder	Springer International Publishing AG	
Author	Family Name	**Amin**
	Particle	
	Given Name	**Atif**
	Suffix	
	Division	
	Organization/University	Dubai Statistics Center
	Address	Dubai, United Arab Emirates
	Email	atif_amn@hotmail.com
Corresponding Author	Family Name	**Valverde**
	Particle	
	Given Name	**Raul**
	Suffix	
	Division	Department of Supply Chain and Business Technology Management
	Organization/University	Concordia University
	Address	Montreal, QC, Canada
	Division	
	Organization/University	CONAIC
	Address	Ciudad de México, Mexico
	Email	raul.valverde@concodia.ca
Abstract	A well designed and integrated database used to present risk management information by using a dashboard interface supported by real time risk management data makes it easy for risk managers to reach a full understanding of the surrounding threats and allows them to find the proper and right controls to mitigate them. The chapter presents a case study for a statistics data center that shows that the calculation of total risk at the organization level is possible by using the proposed risk database that supports decision makers when threats hit the organization. The chapter also shows that presenting the risk level on a dashboard viewer makes risk level clearer for a decision maker in a 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.	
Keywords (separated by " - ")	Data centers - Risk management - Dashboards	

Q1

AUTHOR QUERIES

Q1 Please confirm affiliation details for Raul Valverde.

Chapter 3
Using Dashboards to Reach Acceptable Risk in Statistics Data Centers Through Risk Assessment and Impact Analysis

AU1 **Atif Amin and Raul Valverde**

Abstract A well designed and integrated database used to present risk management information by using a dashboard interface supported by real time risk management data makes it easy for risk managers to reach a full understanding of the surrounding threats and allows them to find the proper and right controls to mitigate them. The chapter presents a case study for a statistics data center that shows that the calculation of total risk at the organization level is possible by using the proposed risk database that supports decision makers when threats hit the organization. The chapter also shows that presenting the risk level on a dashboard viewer makes risk level clearer for a decision maker in a 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.

Introduction

In the modern world the term "Business without a Risk" does not exist (D'Souza and Valverde 2015); with the vast development of technology and science where businesses relies on information technology that depends on internet and unsecure network access, it is almost impossible to achieve total security as there will always be a breaches and vulnerabilities that threaten business and cause damages to interest. Risk management becomes a necessity to every modern business, organization owners and decision makers implement it wildly to find hidden threats and

A. Amin
Dubai Statistics Center, Dubai, United Arab Emirates
e-mail: atif_amn@hotmail.com

R. Valverde (✉)
Department of Supply Chain and Business Technology Management, Concordia University, Montreal, QC, Canada

CONAIC, Ciudad de México, Mexico
e-mail: raul.valverde@concodia.ca

J.M. Gómez et al. (eds.), *Engineering and Management of Data Centers*,
Service Science: Research and Innovations in the Service Economy,
DOI 10.1007/978-3-319-65082-1_3

vulnerabilities in their electronic services and systems and to detect risk before its strike. Monitoring risk level is becoming a trend at every organization in order to protect their assets and interests (Nijburg and Valverde 2011) as early detection of threats would help security staff and risk analysts to build countermeasures and controls that can help to discover vulnerabilities over their systems and business (Wolden et al. 2015). With early detection of risk in organizations, this would give enough time to organizations in order to act and save their interests (Almadhoob and Valverde 2014).

A data center is a facility used to house computer systems and associated components, such as telecommunications and storage systems. Although data centers has been readily adopted and implemented in commercial sectors such as the retail environment, its introduction and implementation for statistics purposes has been growing rapidly particular in the financial market and health care sectors (Khan and Valverde 2014).

The research focuses on conceptual understanding of information technology assets, how assets can be classified and categorized and how to be presented in a risk database for a statistics data center.This research primary focuses on designing and building a successful Information Security Management System (ISMS) module that can help statistics data centers the 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, information, Services and company Image)
2. Classify assets (assign access to applications and documents to different levels of management depending on who can access what and when).
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. An ITIL assets management based framework (Assets Managements Database CMDB) for enhancing and maintaining Information security in statistics data centers.

The final result 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.

Literature Review

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 following topics are reviewed:

- Assets
- Threats and Vulnerabilities
- Impact
- Risk management
- Risk Assessment
- Risk Mitigation

Identifying Risks

Identifying risk can be a very complex and hazard process when it comes to IT industry; one must develop an overall understanding of the business and the surrounding environment where every bit and pieces must count.

Common definitions are shared among related standards and researchers as follows:

- *Risk* is the likelihood of a threat agent taking advantage of vulnerability and the corresponding business impact (Harris 2008).
- *Risk* is the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence (Stoneburner et al. 2002)
- Risk is the combination of the probability of events and its consequences (ISO27001 standard)
- Risks can be defined as the probability of unwanted or unexpected event to occur

IT Systems and Services consist of many related components. In order to understand this relationship we must identify these components and dependent entities. Breaking down the service or system into its components would ease the process of specifying assets hierarchy and levels. Components can be hardware, software, connection while entities can be human, operation and organization image; all can be classified as assets. It is important to classify these assets and group them in categories and grade them. In order to clearly identify Risk levels, we need to assign a value to each asset, one of the key steps to perform a security risk assessment is to determine the value of the assets that require protection (Landoll 2006); this is the first step required by any risk assessment.

The second step is to look for surrounding threats and find their impact values over an asset (Landoll 2006). Impact can be severe causing total damage resulting in business failure or can be acceptable and possible to live with (Stoneburner et al. 2002).

Identifying Risks

Risk occurs when threats find their way to business infrastructure and environment and when vulnerability is exploited in order to allow threats to penetrate. Understanding threats and their probability of occurrence is important part of risk management. Measuring impact value on assets and finding its volume help to estimate the amount of damage risk can produce.

Another important issue is to have a quick and fast mechanism to act against threats. Building a system that is intelligent enough to predict when the next impact might take place actually would help business owners to develop a disaster recovery action and improve their business continuity plans.

Risk management consists of three major processes (Landoll 2006):

1. *Risk Assessment:* it identifies assets, threats and risk's impacts and recommends measurements through setting controls.
2. *Risk Mitigation:* the processes of accepting, avoiding or transferring risk
3. *Risk evaluation and Assessment:* the process of ongoing risk evaluation

Achieving total security is impossible to reach; this issue has been the debate of many organizations especially those who are involved in military and government activates where security measurements are at the top of their priorities. It is not possible to provide total security against every single risk, but it is possible to provide effective security against most risks (Calder and Watkins 2008).

"No system or environment is 100 percent secure, which means there is always some risk left over to deal with" (Harris 2008). Residual Risk can be defined as "The values of risk remaining after security measures have been applied—namely, the risk that remains after mitigation (countermeasures) has been applied" (Kouns and Minoli 2010).

The Term *Residual Risk* is used as the acceptable level of threat that organization can bear and survives with. It is the acceptable level of threat organization must live with in case of no controls and measures are applied or cannot be applied.

To distinguish Residual Risk from Total Risk, Harris (2008) clarifies it in the next formula.

$$\begin{aligned} &\text{threats} \times \text{vulnerability} \times \text{asset value} = \text{total risk} \\ &\left(\text{threats} \times \text{vulnerability} \times \text{asset value}\right) \times \text{controls gap} = \text{residual risk} \end{aligned} \tag{1}$$

Harris (2008) also illustrates Residual Risk as:

$$\begin{aligned} &\left(\text{threats,,vulnerability,and asset value}\right) = \text{total risk} \\ &\text{total risk} - \text{countermeasures} = \text{residual risk} \end{aligned} \tag{2}$$

Accepting part of risk is a process every organization must live with, it is only relevant to how much can be accepted. Sometimes the results of cost benefit analyses indicates that the cost of countermeasures are higher and more expensive than

assets that needs to be protected which give the organization no choice but to live and accept this level of risk. Eventually the question that always rises is what degree of residual risk is acceptable to the organization. Organizations must set this level clearly after risk assessment in order to monitor and observe risk level.

Asset's Attributes for Risk Database

Assets are organization's owned information, or any valuable entities that organization's business depends on. They can also be defined as the property of organization or person. In order to conduct an efficient risk assessment, a classification and categorization of assets are to be conceited and to be well identified. To build a solid design for a risk database many assets dependencies are to be well considered, identified and analyzed. An asset does not refer always to a tangible entity such as hardware or document but it can be none tangible as organization's image, service or a process. It is quite important for the database design to define asset types and subtypes attributes.

Assets types can be as follows:

- Information Assets (electronic files, Data and manuals)
- Paper and hardcopy documents (contracts, Manuals, plans, agreements, correspondences)
- Software assets (applications, systems, codes, Operating Systems)
- Physical assets (Computers, Storages, Network Devices, Cables, RAKS, Power and Cooling Devices)
- People (technical staff, Customers and Clients)

Assets subtype (as proposed in risk database) can be a subcategory of Asset Types, an example of this:

1. Physical asset (Server 004001)
2. Physical asset (Firewall 004005)
3. Information asset (Electronic File 001001)

Assets classification is the act of grouping assets into levels based on their sensitivity and importance to organization. It is useful to categorize or classify assets to organize asset protection requirements, and the vulnerability assessment of assets (Landoll 2006). Some assets might be vital to certain organizations while they are not to others, also classification process can be changed with time, some assets might be top confidential at certain period of time while they can be public at other time. A proposal to win a contract that contains important financial data is very sensitive and classified through bidding while it can be worthless after the bid time is over.

Classification of assets depends on organization methodologies of how its scales and leverage its assets and it can be classified according to different levels. In order to manage and control access to assets, a level of accessibility need to be created

where it will govern who assess what. The business owner of an application (and any related data) must define who will have access to that application and, in terms of any data within it, at what level (i.e. read, write, delete, execute) (Calder and Watkins 2008).

Business applications and IT Systems usually consist of many interrelated assets working and communicating together to host business services. Applications like CRM and ERP solutions usually consist of databases, application and web servers and each hosts an operating system, applications and other software communicating though network and filtered by firewalls and network appliances and governed by network core switches via VLANs.

Failure of any asset item might put the service under risk. Some assets can be servers hosting software and data while others are communication channels allowing this data to flow in and out. Eventually each is important to organization. We cannot say one is more important than other, but we definitely realize that losing data storage is more serious than losing communication between two ends, even though both will result in service failure.

To keep assets under observation and monitoring a good management procedure is required. In order to do this the following is to be considered:

- Storage repository to be used as inventory system for these assets. Asset management includes knowing and keeping up-to-date this complete inventory of hardware (systems and networks) and software (Harris 2008).
- To keep good track of assets Configuration Management Database (CMDB) and Assets inventory are to be synchronized in order to keep track of changes and incidents and vulnerabilities (Harris 2008).
- A well defined asset lifecycle and history process starting at requesting and purchasing the asset and ending with assets termination or write-off.

Assets inventory is the source of Risk Management Systems for the determination of assets types, categories, classifications and values that would help to understand their possible threat and eventually propose the proper control. Based on ISO27001 best practices information assets are to be well identified at risk assessment. The asset inventory should identify each asset, including all the software, and describe it or provide such other identification that the asset can be physically identified (wherever possible, it makes sense to reuse whatever fixed asset number has already been allocated) and full details (including maker, model, generic type, serial number, date of acquisition and any other numbers) included in the inventory (Calder and Watkins 2008).

This process can be carried during risk assessment where result can always be compared with organization logistics register. On the other hand many configuration management applications can provide similar information and can be considered as good source of Information Assets inventory.

Incident Management Systems Assets inventory can be a good source to Incident Management System where the last must be updates each time new assets are added, changed or removed.

ITIL CMDB Information Technology Infrastructure Library's Configuration Management Database is also a good example, it is a container and storage for most information assets used in incidents, change and configuration management. A Risk analyst can use assets information in these systems to evaluate risk assessment and load asset data to their processes. Assets historical information must be also stored and obtained in risk management database. Historical data can be very useful in term of understanding asset's nature like age, value, relationship with other assets, and threats history with impacts. This can result in better evaluation and mitigation of risk.

Asset's owners are Individuals (Organization staff) or Entities (department, Section) which approved management responsibility for asset(s) but has no property rights to assets as they are the property of the organization. All information assets should have a nominated owner ('an individual or entity that has approved management responsibility for the assets') and should be accounted for. (Calder and Watkins 2008).

Assets ownership helps in risk assessment process as owners plays the role of custodian where he/she need to be informed before any changes made to asset. Acceptable use are set of rules and controls made to control access to certain asset such as read, edit, print, email, copy, backup, fax, internet usage and using of organization's mobile phones. Acceptable use addresses employee use of the organization's resources for accessing the information, transmitting or receiving electronic mail, general use of software, and system access (Landoll 2006).

Threats and Vulnerabilities

Threats and vulnerabilities are considered to be the main source of risk, there is no system that is 100% secure. A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability (Stoneburner et al. 2002). The potential for a "threat source" to exploit (intentional) or trigger (accidental) a specific vulnerability (Stoneburner et al. 2002) are:

- Threats usually caused by '*threat source'* where the last can be caused by human or nature, it can be deliberate as in hackings, cyber attacks or accidents as human errors, neglecting and lack of training.
- Risk does not occur when a threat source finds no vulnerability,

Threat is the potential to cause damage and harm to organization asset(s), or the reasons behind threats to occur, example of threat source is a human which might cause harm to an asset though computer attacks and unauthorized access.

A threat-source is defined as any circumstance or event with the potential to cause harm to an IT system (Stoneburner et al. 2002). Breaking threats into categories helps to understand them deeper and identify their threat source. The likelihood of threats to occur is considered as important as threat themselves, some threats might impact once a year while others every hour, this parameter

(Probability of Occurrence or Likelihood of Occurrence or Likelihood Determination) is to be considered in risk evaluation and assessment.

The terms "Likelihood threat occurrence" or "The probability of threat to occur" are both used to identify the number of times threats might occur. Such information can be gathered from threats surveys, historical system attacks and other source of threats. Based on references (Harris 2008) and (Tan 2002) both qualitative and quantitative risk analysis uses these indicators in risk assessment. Vulnerabilities are weakness in organization security or can be considered as gap that threats can penetrate causing impacts on its assets and business (Stephens and Valverde 2013).

It can "leave a system, or asset, open to attacks by something that is classified as a threat, or allow an attack to have some success or greater impact" (Calder and Watkins 2008).Vulnerabilities can also be defined as situations and gaps that if not controlled or maintained will cause an actual threat. With the fast growing of technology and the demand of new software, threats will always find vulnerable entity or area to practice its impacts and attack. Vulnerability sources could be technical, initiated by human or process. The following could be a good source of vulnerability:

- Previous risk assessment
- Vendor's bugs list and reports
- Previous Incident reports generated by helpdesk system (if exist)
- Quality control testing documents
- Scanning tools and conducting penetration test.

Impact Analysis

Impact is the volume of damage that result from uncontrolled threat; impact can be estimated and predicted even before it occurs, where it can effect organization's business, operations and even reputation. Measuring impact is a major step in risk assessment, it aims to measure impact volume against asset's confidentiality, integrity and availability (CIA) through identifying impact's magnitude and source and investigating organization's sensitive and critical information, as a result impact analysis should assign a weight to impact where risk values is to be calculated. IT Governance-ISO27001 refers to Impact as "The successful exploitation of vulnerability by a threat will have an impact on the asset's availability, confidentiality or integrity". These impacts should all be identified and, wherever possible, assigned a monetary value based on the cost to the organization of that attribute being compromised" (Calder and Watkins 2008).

Impact can result in damaging and delaying of the following:

- Organization's every day operations.
- Financial loses which results in loss of assets and liabilities.
- Organization's reputation which is considered a major threat.

Impacts that affects assets can vary in magnitude, it is very important to understand and measure the amount of damage a certain impact might cause to systems and services, and how much time and money will be lost and more important is how many times the impact will occur (Likelihood of occurrence/(ARO)). A fast way to explore threats impacts is by identify their critical business processes (related to their core business). Failure of these processes will cause a critical and vital damage to organization.

Controls

They are set of measurements, activities applied to eliminate, minimize or transfer threats.

"Means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be administrative, technical, management, or legal in nature" (Kouns and Minoli 2010). ISC2 a leaders in information technology describes types of controls as following (Table 3.1):

Controls also can be implementing sets of operations and procedures to improve security measures or adding new protection asset such as purchasing firewall, antivirus or others.

Research Approach

Risk Management

This research used a case study research method where data was collected from primary and secondary data sources. A case study "involves the investigation of a particular situation, problem, company or group of companies" (Dawson 2009). Secondary data, or supporting data, was collected from related books, journals, online 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 know risk management methodologies,

Table 3.1 Controls types

Control type	
Detective	Capable to detect threats like IPS, CCTV
Directive	Administrative tasks and policies
Preventive	Prevent threat to occur like IPS, firewall
Corrective	Identify and minimize threat's impacts like applying security policy
Recovery	Controls that associated with disaster recovery and business continuity processes

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 is based on three processes and their sub processes or steps:

   - Risk Assessment
   - Risk Mitigation
   - Evaluation and Assessment

2. IT Governance, A manager's Guide to Data Security and ISO 27001/ISO 27002 is based on well defined activates supported by template documents which can be modified to fit any organization's Information Security Management System ISMS requirements, it is based on the following:

   - Gap Analysis
   - Identify criticality: the relationships between assets and Objectives
   - Identify potential threats and vulnerabilities (likelihood)
   - Risk Treatment Plan and the selection of controls and statement of applicability
   - Measures of Effectiveness

Based on NIST 800-30 best practices the following figure illustrates risk assessment processes describing inputs and outputs entries (Fig. 3.1).

Information Gathering Methods and Tools

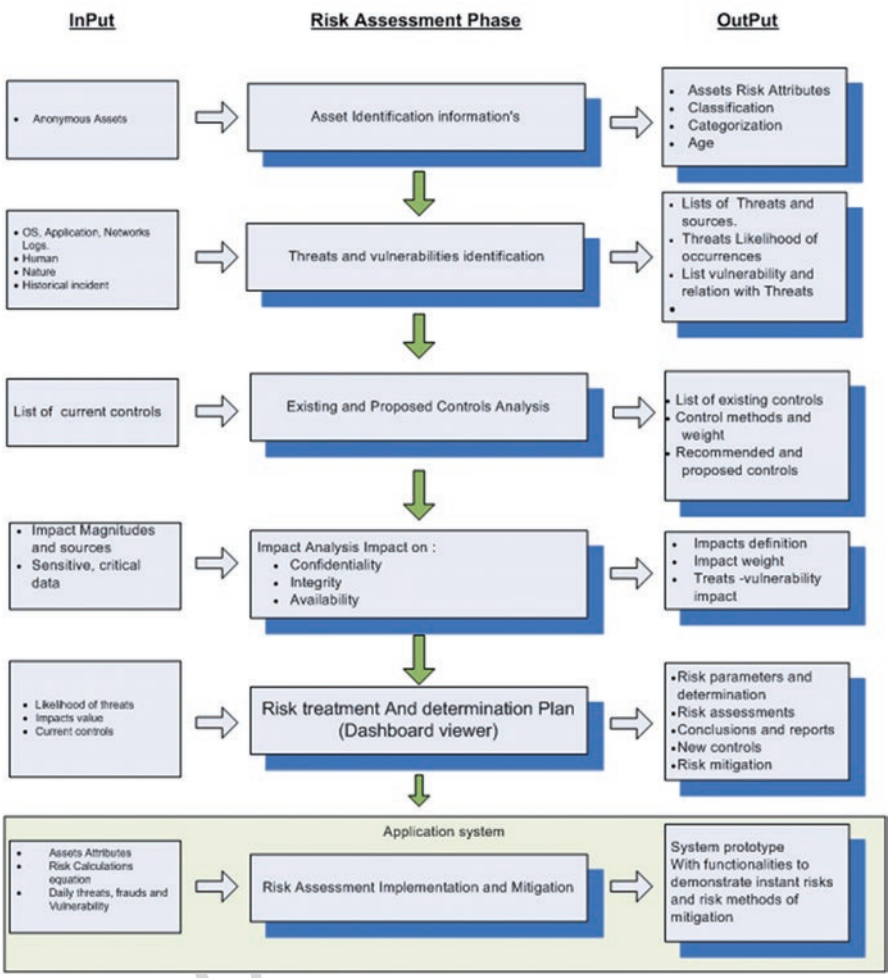
When gathering data, it is quite important to define WHAT is to be collected, and WHO are the involved entities and parties in this process and HOW to collect data.

Before starting the risk assessment, it is important to identify what is to be collected. The following is to be considered:

- Assets data (types, Categories, Classifications, Owners, History data)
- Threats and Vulnerabilities (details description, categories, sources, types, remedy actions, number of occurrences)
- Impacts (details of threats impacts)
- Controls information (description types such as asset, plan, process, prices)

As part of the data collection requirements, it is important to identify the people that can help to speed the process of data gathering as hearing their opinions from different points of views (technical and business) and blend them in one container will help to discover many hidden issues. The process emphasizes on carrying a sequence of interviews with asset's owners, stakeholders, technical teams and risk related organization's members; The interview itself can result in an incredible amount of information if it is conducted properly (Landoll 2006).

The following stakeholders and organization's staff are involved in this process:



this figure will be printed in b/w

Fig. 3.1 Risk assessment phases based on NIST SP 800-30

- Assets owners
- System and network Administrators
- Database Administrators
- Information Security specialist/Officer
- Business Owners
- Risk Manager/Team (if available)
- Financial Manager
- Top Management

Conducting an interview is considered to be an effective way of data gathering, it allows direct interaction with stakeholders, technical staff and top management,

read their impression and understand their concerns not to mention the short time invested in this process. When conducting an interview, it is possible to address any confusion immediately, which minimizes the time lost and the frustration experienced by both sides (Wheeler 2011). Interviews to key personnel help to determine their ability to perform their duties (as stated in policies), their implementation of duties not stated in policies, and observations or concerns they have with current security controls" (Landoll 2006).

Questionnaire is just a passive version of an interview (Wheeler 2011). Questionnaires must be designed in a smart way to cover all to risk assessment process requirements that can be considered as a good input to the risk database for this research. 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 following templates are to be used

(i) Collecting Assets Information using:

  (a) *Assets Classification and Categorization Template*.
  (b) *Assets Information Details from Inventory System.*

(ii) Collecting threats and vulnerabilities Information using "*General Threats Identification Sheet*"
(iii) Collecting existing controls using: "Controls" template
(iv) Collecting Impact Analysis details using:

  (a) *Qualitative Risk Assessment Template*
  (b) *Quantitative risk assessment templates*

Qualitative Risk Assessment Methodology or Approach

In order to scale assets not based on its marketing value but on its importance to the organization, interviews with business owners were conducted and templates evaluated by related members. The following Table 3.2 describes how assets are evaluated based on business sensitivity's best practices at Dubai Statistic Center.

There are other parameters govern assets values which need to be considered also when rating an asset (Table 3.3).

Considering the above information and feedback from interviews and questionnaires the following rating is considered (Table 3.4):

Besides assets' data threats information must be well identified and collected in order to correctly weight their impact values. Threats must be identified, classified by category, and evaluated to calculate their damage potential to the company

Table 3.2 Assets values based on qualitative approach/Dubai Statistic Center t2.1

Assets values	Description	t2.2
High values assets	Assets involved in core business, stalling or losing them will compromise organization CIA and would result in severe impact and losses such as financial and reputation wise which is unacceptable. An example of this losing organization sensitive information, damaging and ruin its profile	t2.3 t2.4 t2.5 t2.6 t2.7
Medium value assets	Any assets that are not part of core business and do not cause a threat to the organization image, impact can be bearable and acceptable Example attendance system, development server and others similar.	t2.8 t2.9 t2.10
Low value asset	Loosing or staling such assets would not compromise organization's CIA and would result in miner disruption Example printer, scanner, telephone device and others similar.	t2.11 t2.12 t2.13

AU4

Table 3.3 Other parameters effecting assets t3.1

Asset parameter	Description	t3.2
Assets dependency level	Referencing asset's hierarchy and relationship with other assets. Is the asset depending on other assets? (application installed on app server) Does it have children (dependencies)? The more children an asset has, the higher its value as other assets depends on it. (server that hosts different software and data bases should worth more to the organization than a server with a single software that is installed on it)	t3.3 t3.4 t3.5 t3.6 t3.7 t3.8 t3.9 t3.10 t3.11
Assets access level/classifications	What is the classification level for this asset? Is it top classified where losing the asset will damage the organization's reputation or it is public and can be compromised?	t3.12 t3.13 t3.14 t3.15
Asset age	Represent the number of years that the asset is operating.	t3.16 t3.17
Conclusion: in order to assign a value to asset (high, medium, and low) the above parameters are to be considered.		t3.18 t3.19 t3.20

(Harris 2008). Based on best practices at Dubai Statistic Center threats data can be gathered from the following sources: 413 414

- Historical systems attacks 415
- World wide data 416
- Surveys and Questionnaires 417

Threat's historical data can be a good reference to organization's Information Security procedures, it can shows systems and services historical failures and what are the measures taken (if exist) to protect against such threats. This can be treated as the starting point of threats gathering. 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 418 419 420 421 422 423

t4.1 **Table 3.4** Qualitative asset
t4.2 rating

Asset value	Rate
High	3
Medium	2
Low	1

t4.3 t4.4 t4.5 t4.6

t5.1 **Table 3.5** Probability or likelihood of threat to occur

Likelihood of threats occurrence	Description	Weight
Negligible	Unlikely to occur	
Very low	Might occur few times every 5 years	
Low	Like to occur once every year	0.1
Medium	Occurs once every 6 months	0.5
High	Occur multiple times per month	1
Very high	Multiple times every week	
Extreme	More than once every day	

t6.1 **Table 3.6** General threats list

Threat	Probability of occurrence	Existing control	Applicable assets	Owner
Document theft	Medium	Personal lockers	Bids Technical proposals Technical manuals	System admin Network admin Sales department
Fire	Low	Fire distinguisher	Data Center IT department	Operation section IT department
Power failure	High	UPS Generators	Data Center	Operation section

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). Based on meetings results with Risk Manager and referencing NIST SP-800-30 (Stoneburner et al. 2002), threats likelihood of occurrence can be measured as following (Table 3.5):

Identifying the common well known threats is an easy way to start collecting threat information. Table 3.6 presents common threats data that can exist at most of IT departments.

It would be better to identify major threats over major assets to save time and efforts. Based on asset value to organization and interviews conducted with (Risk Manager, asset's owners), this research measured the impact volume according to its power to stole business or interrupt it. Referencing NIST SP 800-30 (Stoneburner et al. 2002) and based on the Dubai Statistic Center, business sensitivity in the following Table 3.7 illustrates impact volume measurement.

Table 3.7 Impact volume Measurements based on NIST SP 800-30 t7.1

Impact volume	Description	t7.2
Insignificant	Almost no impact if threat and vulnerabilities are exploited	t7.3
Minor	Minor effects on organization's assets and business, recovering is manageable	t7.4
Significant	Results in some tangible damage, and require some time to recover (example internal service interruption and restored, connection down restored immediately)	t7.5 t7.6 t7.7
Damaging	Noticeable impact that result in large but internal damage, requires time and resources to restore (example internal operation failure)	t7.8 t7.9
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)	t7.10 t7.11 t7.12

t8.1 **Table 3.8** Impact values

				t8.2
Critical	High	H	3	
Damaging	Medium	M	2	t8.3
Minor	Low	L	1	t8.4

Based on the previous table, impact values can be presented as following (Table 3.8): 438 439

This approach is based on giving a weight value 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 follows (Harris 2008): 440 441 442

$$\text{Risk} = \text{Asset Value} \times \text{Impact} \times \text{Likelihood of Threat} \quad (3)$$ 443

Quantitative Risk Assessment Methodology 444

In order to gather monetary risk values where assets values are measured in currency, the finance manager and involved team in asset evaluation are to fill a Quantitative Risk assessment questionnaire. Based on interviews with Assets Owners, Financial Manager and Risk Manager, the followings points are to be considered: 445 446 447 448 449

Financial Cost: 450

- Market Cost 451
- Development Cost (in case of Application Software) 452
- Installation and Configuration Value 453
- Maintenance and Support Cost 454
- Replacement Cost 455
- Operation and running Cost (electricity, License in case of software) 456
- Depreciation Cost 457

458 Non Financial Cost

459 • Value to organization (like Organization Reputation)
460 • Asset value to users and customers

461 Based on previous assets parameters provided, the following formula can be gen-
462 erated and used to set quantitative value to asset.

$$\text{Asset Value} = \text{Purchasing Value} - \text{Depreciation value} + (\text{cost of time to recover}) \text{ or cost to replace asset and put it to functioning} + \text{loss caused by service stopping} + \text{Support and Maintenance value} \quad (4)$$

463

464 The *exposure factor (EF)* represents the percentage of loss a realized threat could
465 have on a certain asset (Harris 2008; Kouns and Minoli 2010). Single Loss
466 Expectancy (SLE) is the total amount of revenue that is lost from a single occur-
467 rence of the risk (Kouns and Minoli 2010). Annual Rate of Occurrence (ARO) is the
468 normalized rate at which the risk exposure resulting in actual damage occurs during
469 1 year (Kouns and Minoli 2010).
470 The *annualized rate of occurrence (ARO)* is the value that represents the esti-
471 mated frequency of a specific threat taking place within a one-year timeframe
472 (Harris 2008). Qualitative risk is based on assigning monetary value to assets. Based
473 on Harris (2008), Tan (2002) and Wheeler (2011) the quantitative risk formula in
474 the proposed risk database is calculated as below:

$$\begin{aligned} &\text{Single Loss Expectancy}(\text{SLE}) = \text{Asset Value}^{*}\text{Exposure Factor}(\text{EF}) \\ &\text{Annual Loss Expectancy}(\text{ALE}) = \text{SLE} \times \text{Annual Rate of Occurrence}(\text{ARO}) \end{aligned} \quad (5)$$

475

476 Data for the proposed dashboard viewer can be presented as:

477 • Charts
478 • Tables

479 The proposed study case template to analyze risk data is presented below in
480 Table 3.9.

t9.1 **Table 3.9** A proposed study case template to analyze risk data and propose action

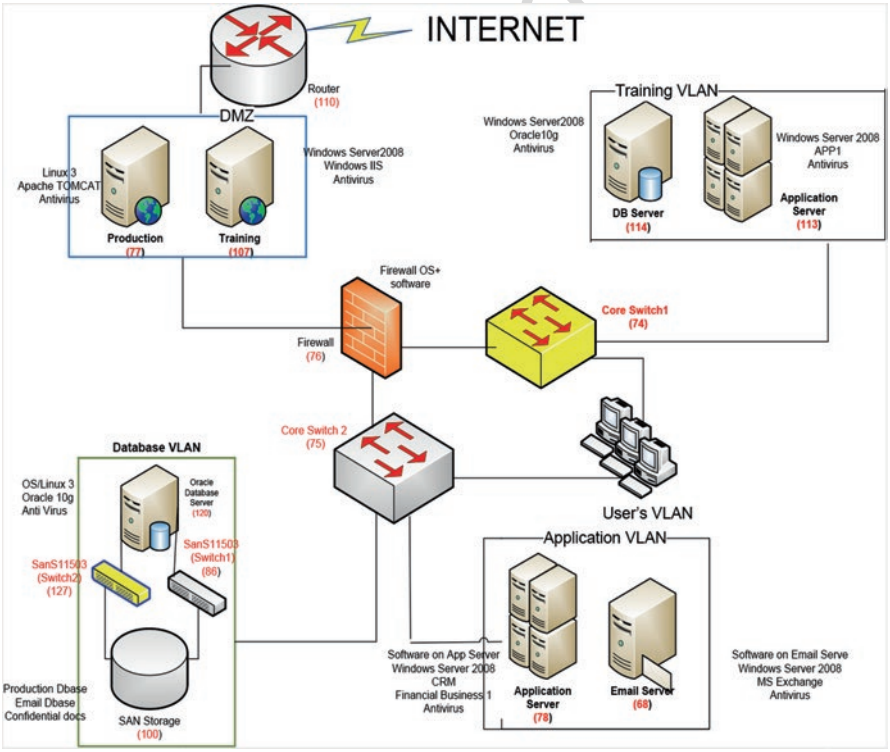
t9.2	Case #	
t9.3	Name	The case description or the criteria title
t9.4	Indicators	How this case was explored? What are the risk indicators?
t9.5 t9.6	Effective parameters	What are the related parameters? Example asset value, impact value.
t9.7	Searching criteria	What is the searching criteria, what to look for and where?
t9.8 t9.9	Analysis and investigation	This section covers analyzing the case (HOW?) and what indication we need to build our decision on?
t9.10	Decision and action	Decision and action need to be taken.

Case Study and Data Collection

In order to present risk data accurately at any organization, the risk team must have a full picture over organization's main services and its backbone infrastructure where every asset (tangible and none) software and hardware is identified. The above figure demonstrates an IT based service with four VLANs (Virtual Local Area Network) similar to the environment of the Dubai Statistic Center and its components of hardware and software as they are described in details in Fig. 3.2.

A good understanding of the organization structure leads to a better identification of threats and vulnerabilities areas. The risk team can develop a solid idea on how to plan risk management processes, contacting whom in case of failure, which departments and sections will be out of business in case of threat's impact and what are the losses.

Figure 3.3 represents part of the Dubai Statistic Center's Departments Organization Chart. Top management approval must be granted before initiating a risk assessment process, the following should be considered:



this figure will be printed in b/w

Fig. 3.2 IT service infrastructures

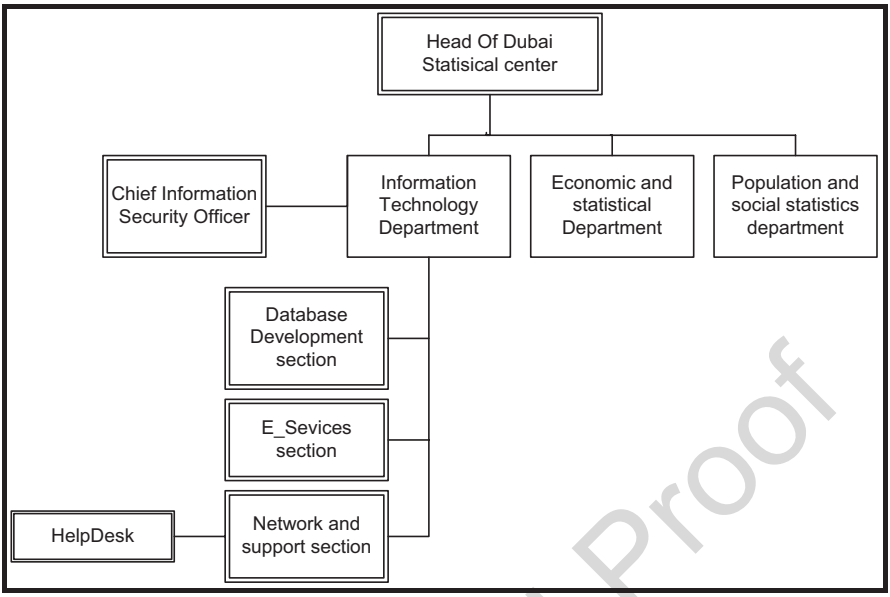


Fig. 3.3 Dubai Statistic Center Organization chart

- All related stakeholders are to be notified.
- All proposed templates, questionnaires and interviews scenarios are to be checked and approved.
- Business owners and technical staff are to be notified.
- Checking that the inventory system is up to date and contains all assets information required for the assessment.

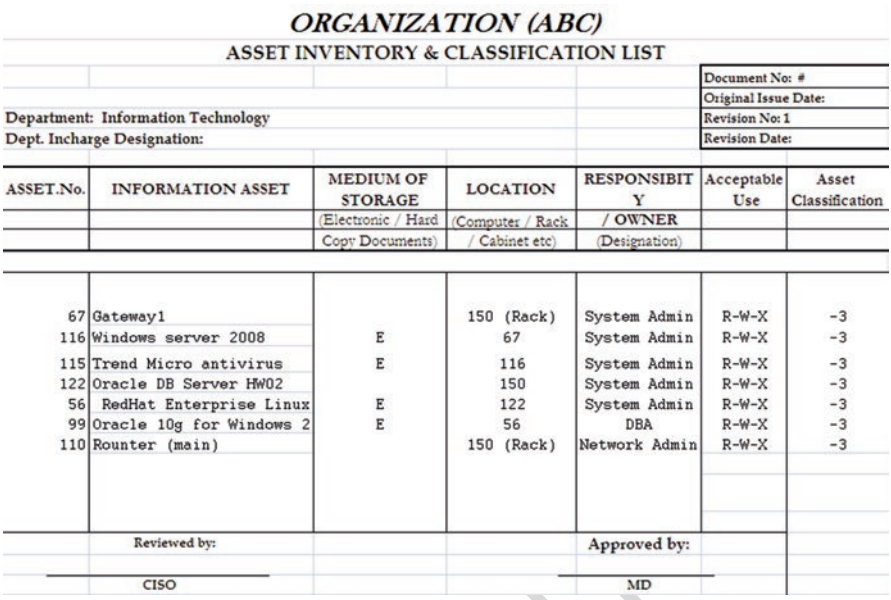
The following lists all templates and sheets descriptions used for data collection.

- Assets Inventory and Classification List
- Threat Information Collection Form
- Controls
- Qualitative Risk Assessment data
- Quantitative Risk assessment data

As a result of top management and stakeholder's approval of proposed templates, all questionnaires and Templates were distributed to related sections and individuals. Also, interviews should be conducted with related department members and managers.

Assets Information Identification

The first step in assets gathering is to collect assets' data based on its importance to the organization where assets' type, nature, mean of storage, owner and access privileged are to be considered. The first step is to define the scope of the effort.



ORGANIZATION (ABC)

ASSET INVENTORY & CLASSIFICATION LIST

Document No: #	
Original Issue Date:	
Revision No: 1	
Revision Date:	

Department: Information Technology

Dept. Incharge Designation:

ASSET.No.	INFORMATION ASSET	MEDIUM OF STORAGE (Electronic / Hard Copy Documents)	LOCATION (Computer / Rack / Cabinet etc)	RESPONSIBITY / OWNER (Designation)	Acceptable Use	Asset Classification
67	Gateway1		150 (Rack)	System Admin	R-W-X	-3
116	Windows server 2008	E	67	System Admin	R-W-X	-3
115	Trend Micro antivirus	E	116	System Admin	R-W-X	-3
122	Oracle DB Server HW02		150	System Admin	R-W-X	-3
56	RedHat Enterprise Linux	E	122	System Admin	R-W-X	-3
99	Oracle 10g for Windows 2	E	56	DBA	R-W-X	-3
110	Rounter (main)		150 (Rack)	Network Admin	R-W-X	-3

Reviewed by: CISO

Approved by: MD

this figure will be printed in b/w

Fig. 3.4 Assets Inventory and Classification List (AICL)

In this step, the boundaries of the IT system are identified, along with the resources and the information that constitute the system (Stoneburner et al. 2002).

The second step is to collect assets' information based on its logistic storage where assets' details are to be recorded like serial No#, brand, maintenance contract details and others. The logistic information is easy to get from any assets inventory system or Configuration Management Database CMDB. Collected data can be pushed later to a risk database depending on how the organization plans to automate this process (Fig. 3.4).

Based on the above template and the Dubai Statistic Center Infrastructure in Fig. 3.2, the data collected was based on:

- Storage media
- Physical Location
- Owner
- Acceptable Use and many
- Asset Classification

The required risk information and data are collected and coded using the proposed excel sheets as to be used later to feed the risk database. Figure 3.5 shows the excel sheet for asset information.

	Ast_ID	Ast_Desc 119	Ast_Serial_no	Ast_Model_no	Ast_Brand	Ast_Category	Ast_Service	Ast_Type	Ast_SubType	Ast_Classification	Ast_Access_level	Ast_Qltv_Value	Ast_Age	Ast_Qntv_Value	Ast_SuppCont_type	Ast_SuppCont_Duration	Ast_SuppCont_DateF
1																	
2	110	Rounter (main)	xyz	Rt987	15	1	1	1	24	1	-3	3	3	5000	2	2	7/22/2010
3																	
4		DMZ															
5	77	Application server_HW01	APP1212X44L	3560	1	1	1	1	1	1	-3	3	3	5600	2	1	1/1/2011
6	56	RedHat Enterprise Linux Release 3		linux Operating Sys	11	1	1	2	1	1	-3	3	4	2000	2	2	1/22/2010
7	109	Apachi TOMCAT SW	Tmyvc		11	1	1	2	5	1	-3	3	3		1	1	1/1/2011
8	3	Trend Micro Antivirus _Linux	Ant L679		2	1	1	2	2	1	-3	3	1	3800	2	2	1/12/2010
9																	
10	107	Training server_HW02	APP1212X44L	3560	1	1	1	1	1	1	-3	3	4	5600	2	1	1/1/2011
11	37	Win Srv 2008 SW	Tmyvc	Windows Server	4	1	1	2	1	1	-3	3	3	2000	1	3	1/12/2010
12	108	Win Srv IIS SW	Tmyvc	Windows	4	1	1	2	3	1	-3	3	3		1	3	1/12/2010
13	105	Trend Micro Antivirus _Windows	Ant W2345		2	1	1	2	2	1	-3	3	1	2000	2	2	1/12/2010
14																	
15	76	ASA 5520	fir1212X47sF	5520	15	1	1	1	20	1	-3	3	4	14000	2	1	1/1/2011
16	84	OS Firewall	JMX16Z0RK	abc	15	1	1	2	1	1	-3	3	4		2	1	1/1/2011
17																	
18	74	SWITCH -Core01	Sxy12050166	4503	15	1	1	1	5	1	-3	3	4	12000	2	1	1/1/2011
19		VLAN Training															
20																	
21	113	Training APP server_HW03	APP1212X44L	3560	1	1	1	1	1	1	-3	3	4	5600	2	1	1/1/2011
22	114	Win Srv 2008 SW	Tmyvc	Windows Server	4	1	1	2	1	1	-3	3	3	2000	1	3	1/12/2010
23	106	CRM Software_TSW	App software 1		70	1	1	2	3	1	-3	3	2	25000	2	1	1/1/2011
24	115	Trend Micro Antivirus _Windows	Ant W2346		2	1	1	2	2	1	-3	3	1	1800	2	2	1/12/2010
25																	

Fig. 3.5 Asset information after coding

Conrtols Information

Control_ID	Asset Id	Control_Desc	Control type	control_est_market Price
0		No control on the asset	0	
1	1	Trend Micro - windows	4	
4		valid Maintenance Contract	4	
29		Using Change Management Procedure	4	
30		Purchase and Install a new san switch	4	15000
92		Purchase UPS	1	2000
95		Intrusion detections 360	1	35000
5		ASA-5520 (Primary) logs	1	
6		Access Control Policy	2	
8		Disable ftp port	4	
9		Disable ssh port	4	
12		monitor Alert logs	2	
13		Miror Local Disks	2	
14		regular System Backup	2	
15		Hire Qualified DBA	4	
16		Provide Redundent Server?Cluster	4	
17		Update Firewall Configuration	4	
28		Install IPS	4	

Control_id is a sequeces code

Control type : 0 no control 1 Asset 2 Process 3 Plan 4 Action

Fig. 3.6 Evaluating control template

Collecting Controls Information

An interview to technical and business staff can help to identify what controls currently exists, this process helps the risk the team to highlight the current available countermeasures. Based on best practices and interviews conducted with related members and business owners, the following proposed template in Fig. 3.6 is used to gather existing controls applied to certain assets

Collecting Controls Information

Based on the risk formula and previous data collected via assets, threats and controls templates, the following table is produced with risk values against assets before and after the proposed controls (Fig. 3.7).

Collecting Quantitative Risk Data

Based on risk formula and previous data collected via assets, values, threats and expected loss factors, a table with risk values in Fig. 3.8 illustrates the calculation of risk values against asset before and after proposed control.

The template gathers assets information based on asset's financial cost to organization, the calculation formula can be complex and vary from asset to another.

Document No : DSC-02
Date of Issue : 08/10/2010
Revsion No
Date of Revision

Section : Information technology_
Section Head : _____

Asset Info									Controls Detail			
seq	asset Id	Asset Description	Date	Asset Value (H,M,L)	Threat_id	Threats description	Impact Value (H,M,L)	status Control	Control_Id	Control Description	Probability of threat	Risk Value
1	86	SanS11503 (Switch 1)	5/10/2011	3	38	Non redundant SAN Switches	3	0	0		2	9
2	86	SanS11503 (Switch 1)	5/23/2011	3	38	Non redundant SAN Switches	2	5	30	puchase and install san switch	1	0.6
3	74	SWITCH -Core01	3/18/2011	2	40	Electrical PS. failure	2	0	0		3	4
4	74	SWITCH -Core02	3/18/2011	2	40	Electrical PS. failure	2	5	92	Intrusion detections 360	0	0.4
5	100	IBM SAN Storage	2/17/2009	3	25	Unauthorized access	3	0	0		4	0.9
6	101	IBM SAN Storage	2/18/2009	3	25	Unauthorized access	3	0	0		6	4.5

control Status : 0 current 5: proposed

this figure will be printed in b/w

Fig. 3.7 Qualitative risk assessment

Document No : DSC-02
Date of Issue : 13/10/2010
Revsion No :
Date of Revision :

Section : Network and support section
Section Head : XXXXX

Asset Info										Controls Detail			
seq	asset Id	Asset Description	Asset Value $	Threat_id	Threats description	DATE	Expected lossfactor (EF)	Single Loss Expectancy (SLE)	status Control	Control_Id	Control Description	Annual Rate of Occurrence	Risk Value in $
1	86	SanS11503 (Switch 1)	15000	38	Non redundant SAN Switches	5/10/2011	1	15000	0	0	No control	2	30000
2	86	SanS11503 (Switch 1)	15000	38	Non redundant SAN Switches	5/23/2011	0.5	7500	5	30	Purchase and install a new san switch	1	15000
3	74	SWITCH -Core01	25000	40	Electrical PS. failure	3/18/2011	0.25	6250	0	0	No control	3	18750
4	74	SWITCH -Core02	25000	40	Electrical PS. failure	3/18/2011	0.1	2500	5	92	Purchase UPS	0	7500
5	100	IBM SAN Storage	5000	25	Unauthorized access	2/17/2009	0.1	500	0	0	No control	4	20000
6	101	IBM SAN Storage	5000	25	Unauthorized access	2/18/2009	0.1	500	5	95	Intrusion detections 360	2	1000

this figure will be printed in b/w

Fig. 3.8 Quantities risk assessment

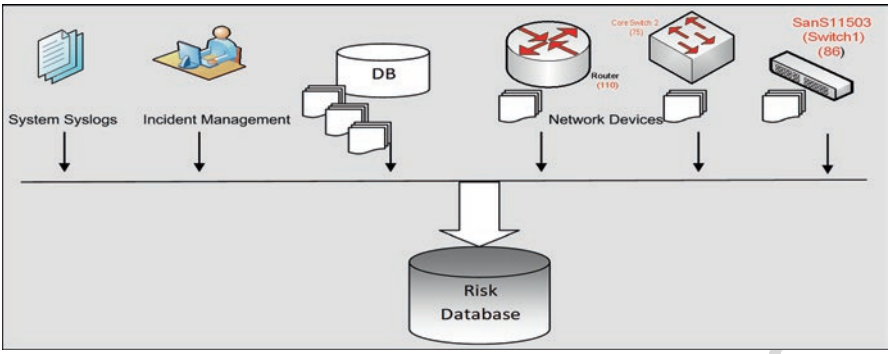


Fig. 3.9 Sources of threats

Collecting Quantitative Risk Data

Threats data can be collected using surveys and from historical incidents. Software logs if interpreted and reformatted can be another good source of threats, they can show what is the real infrastructure and what are the technical threats surrounding the organization. When it comes to security, these logs can be a good reference for vulnerability and penetration test as well. Other advantage of using system's log is to achieve real time views; risk database can log/accept data from various incident sources. Incident Management Systems and SysLog can be a good example for best practice. The following Figs. 3.9 and 3.10 presents electronic threats sources to risk database.

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 previously provided templates the following entities can be identified:

1. Assets
2. Threats
3. Controls

Going further by breaking down the entities into sub entities based on collected data. The following Table 3.10 illustrates the major database tables proposed to present risk data. The table also describes the functionality and purposes behind each database table.

This approach is more practical for some organizations while it is not for others but it is still easier and requires less calculation. It is based on surveys and questionnaires provided and it is more achievable when it comes to rate similar hardware

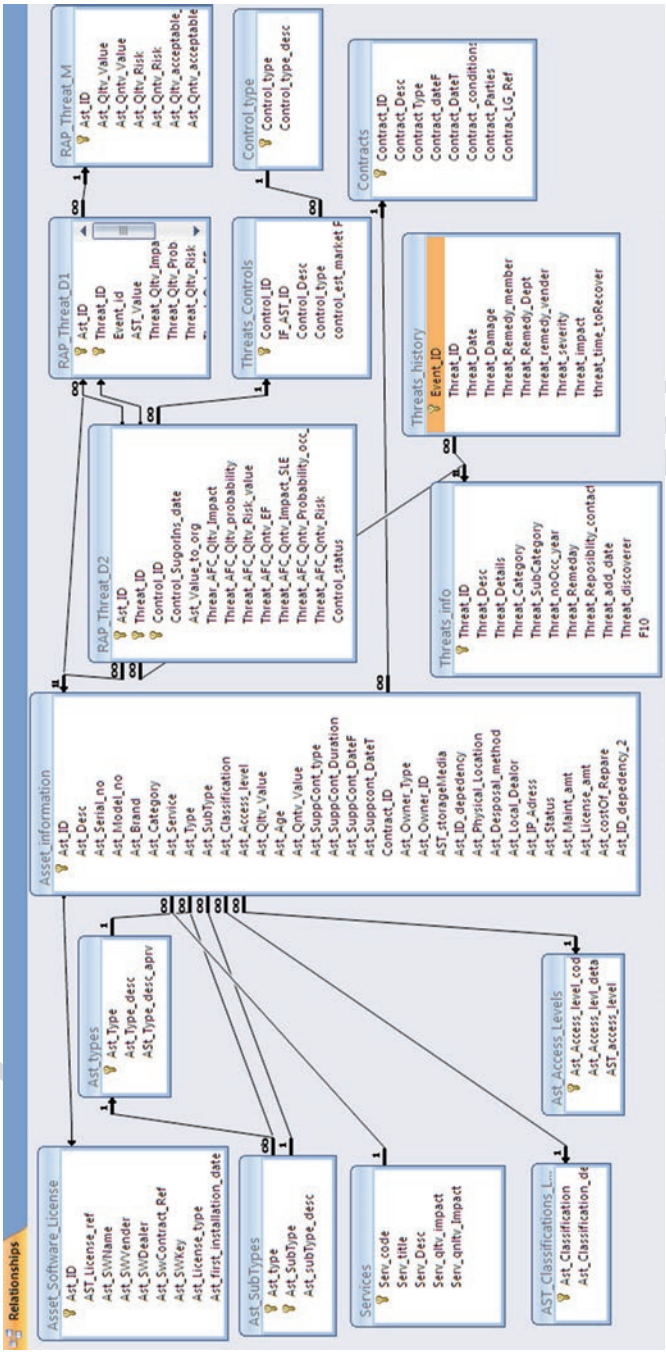


Fig. 3.10 Database design

t10.1 **Table 3.10** Database tables

t10.2 Tables	Description
t10.3 Services	This is the master table that most of the organizations assets is linked to, since any organization has mission and vision to provide the specified services
t10.6 Asset _Information	Master table that contain all required data required about all IT assets to control and monitor at real-time risks such as: Asset id, description, type, subtype, category, value to organization, age which involved directly in calculating the current risk to assets. Other data manages the yearly maintenance contracts, location, disposal methods, and item status if it is active or canceled (write-off). One the fields is Ast_ID dependency which relates the item to its dependencies such as if a server is at risk.
t10.14 Assets_types	Assets types can be information, paper, hard copy, physical, people.
t10.15 Assets_sub_types	Such as server, software, firewall, …
t10.16 Assets_ Classification_ Level	As in Table 3.1 assets access level
t10.19 Threats_info	Table of threats information, threat_ID which will be used as reference for the threat in the database, detailed description of the threat, category (human, technical..), subcategory (power failure..), impact scale (high, medium..), access level (top confidential, mangers, section heads) what is the best remedy, and the person or dept. in charge.
t10.24 Threats_History	Table of threats occurrence history, contains all threats history impacting organization and what was the remedy? Who recovered? And the severity level with the damages caused. The history will be used for data mining that will be displayed if any of the risks occurrences exceeds our expectation and should we add more controls of assets.
t10.30 RAP_Threat_m	Risk assessment plan master table, which has only the final accumulative risk for all assets items after implementing controls.
t10.32 RAP_Threat_D1	A detail table to store all possible threats for each asset and values to organization, impact, possible occurrence and calculated risk used to calculate final accumulative risk.
t10.35 RAP_Threat_D2	A detailed table to store all the controls used to mitigate threats risk's which is stored at RAP_Threat_D1, impact after implementing the control, new possible occurrence and the calculated risk, control status if it is proposed or implemented, or canceled
t10.39 Threats_Controls	A tables to store all used or proposed controls with a reference, description and type of control, since it mostly as asset item also or a new business procedure or new plan.
t10.42 Ast_access_Level	Assets access level as the standard code used to determine the access level to the asset item (top management, manger, head section, inside the organization, or public), it is used mainly for sensitive documents such contract, financial data, and any assets that has limited access only.

574 that exists in two different businesses (example a Server can be rated as HIGH when
575 it comes to production environment while the same Server can be rated as LOW if
576 it is used for training purposes). Table 3.11 presents the risk formula calculation in
577 the risk database based on a qualitative approach.

Table 3.11 Qualitative risk dependencies and calculation method in the proposed database t11.1

Risk dependency	Calculation method	t11.2
Asset qualitative value AST_QLTV_VALUE	In qualitative approach asset is rated as (HIGH, MEDIUM, LOW) and rated as follows HIGH = 3, MEDIUM = 2, LOW = 1)	t11.3 t11.4 t11.5
Threat impact after controls are applied THREAR_AFC_QLTV_IMPACT	Impact value, can be (HIGH, MEDIUM, LOW) and rated as follows HIGH = 3, MEDIUM = 2, LOW = 1)	t11.6 t11.7 t11.8
Probability of threat to occur or take place it can also be called as the likelihood of threat to occur. THREAT_AFC_QLTV_PROB	The frequency of threat to occur LOW—Occurs once every few years and rated as 0.1 MEDIUM- occurs once every 6 months and rated as 0.5 HIGH- occurs once every month and can be rated as 1	t11.9 t11.10 t11.11 t11.12 t11.13 t11.14 t11.15
Qualitative risk (calculated value) THREAT_AFC_QLTV_RISK	Risk is calculated in the proposed database using qualitative approach as follows: RISK = ASSET value * impact value * probability of occurrence	t11.16 t11.17 t11.18 t11.19

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. Table 3.12 shows threats and their single Loss Expectancies, Annual Rate of threat's Occurrences and Annual Loss Expectancies.

Dashboard and Risk Analysis

A dashboard viewer can provide various risk information 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 in order 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
- Tables

Table 3.13 describes the risk scenario 1 that is meant to find high risk based on threat's impact by using a qualitative approach. The risk manager in this case is

t12.1 **Table 3.12** Quantitative risk dependencies and calculation method

t12.2		Formula
t12.3 t12.4 t12.5 t12.6 t12.7 t12.8 t12.9 t12.10 t12.11	Asset quantitative value (AST_QNTV_VALUE)	There are many ways to measure and calculate asset qualitative value Purchasing value Depreciation value Cost of recovery/replacement time Delay and stepping time cost Ast_Qntv_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 cost
t12.12 t12.13 t12.14 t12.15 t12.16 t12.17 t12.18 t12.19	Single loss expectancy (calculated value) Is the quantitative asset value multiplied by exposure factor	Single loss expectancy (SLE) is calculated by multiplying asset quantitative value (calculated in the previous row) by threat exposure factor (EF-the percentage of loss a threat can have over an asset). Example: If asset that worth 20 K is exposed to threat that can damage 30% of the asset such as partial malfunction then single loss expectancy (SLE) = AST_QNTV_VALUE* EF = 20,000 * 0.3 = 6000$
t12.20 t12.21 t12.22	Annual rate of occurrence THREAT_AFC_QNTV_PROB_OCC_ARO	How many time the threat can occur (usually its calculated per year) Value can be between 0 to greater than one
t12.23 t12.24 t12.25 t12.26 t12.27	Annual loss expectancy (calculated value)	This value can tell the management how much damage in monetary value can certain threat annually cause to a certain asset, in other word it is the SLE multiplied by ARO = AST_QNTV_VALUE * THREAT_AFC_QNTV_EF * THREAT_AFC_QNTV_PROB_OCC_ARO

t13.1 **Table 3.13** Scenario 1

t13.2	Scenario # 1	
t13.3	Name	Finding high risk based on threat's impacts/qualitative approach
t13.4 t13.5	Indicators	Risk level (high impact and low probability), (high impact and high probability)
t13.6 t13.7	Effective parameters	Impact Likelihood of occurrence
t13.8 t13.9 t13.10	Searching criteria	Looking for assets or systems with: High impact value and low likelihood of occurrence High impact value and high likelihood of occurrence
t13.11 t13.12 t13.13 t13.14 t13.15 t13.16 t13.17 t13.18	Analysis and investigation	All high impacts values must be taken seriously; IT staff might underestimate risks with low likelihood of occurrence as they might never occur. Example an out of date antivirus on database server, it is a fact that most of database servers are located in a separate VLAN which is isolated from external traffic and the probability of virus attack is very unlikely to occur but that does not mean it is safe to leave the antivirus software out of date. The impact will be very high if the server is attacked.
t13.19 t13.20 t13.21 t13.22	Decision and action	All high impact values are to be seriously considered even with low probability of occurrence. An immediate action is to be taken for any high impact assets even if the probability of attack was very unlikely to occur.

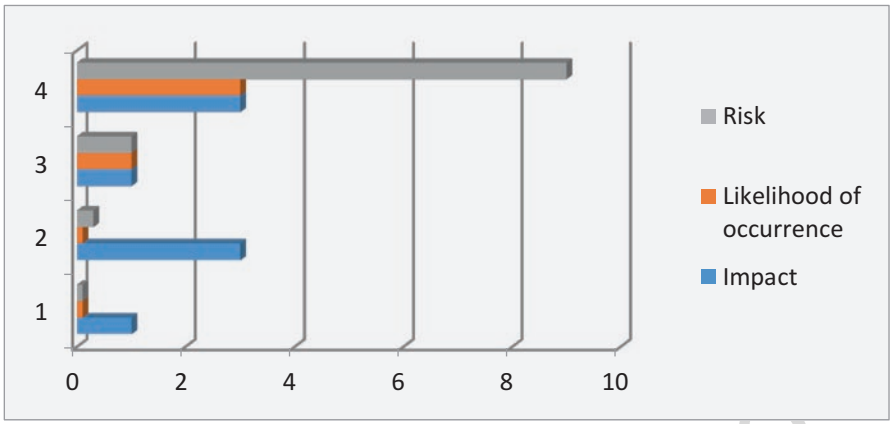


Fig. 3.11 Dashboard view – high risk based on threat's impacts/qualitative approach

Ast_ID	Threat_ID	Event_year	AST_Value	Threat_Qltv_Impa	Threat_Qltv_Probability_occ	Threat_Qltv_Risk	Threat_Qntv_EF	Threat_C	Threat_Qntv_Probability_occ	ARO	Threat_Qntv_Risk
IBM SAN Storage	100	25	2009	3	3	1	9	0.3	1500	2	3000
IBM SAN Storage	100	25	2010	3	3	1	9	0.3	1500	6	9000
IBM SAN Storage	100	25	2011	3	3	1	9	0.3	1500	9	13500
Email MS Exchange Server_	68	25	2009	2	2	0.5	2	0.1	1200	4	4800
Email MS Exchange Server_	68	25	2010	2	2	0.5	2	0.1	1200	6	7200
Email MS Exchange Server_	68	25	2011	2	2	0.5	2	0.1	1200	9	10800
Oracle DBA-Server-HW02	122	25	2011	3	3	1	9	0.1	1700	9	15300
Oracle DBA-Server-HW03	122	25	2010	3	3	1	9	0.1	1700	6	10200
Oracle DBA-Server-HW04	122	25	2009	3	3	1	9	0.1	1700	4	6800

Fig. 3.12 Dashboard view—risk values

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 Fig. 3.11.

Risk Scenario 2: Decisions Based on Historical Risk Data

Risk historical data can be a good 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 Fig. 3.12.

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 Fig. 3.13.

Figure 3.14 shows a dashboard view that indicates that IBM SAN Storage, MS Exchange Server and Oracle Database server are subject to "Unauthorized Access". This threat is increasing every year.

		25 Unauthorized access		
			quantitattive	
		2009	2010	2011
IBM SAN Storage	100	3000	9000	13500
Email MS Exchange Server _	68	4800	7200	10800
Oracle DB-Server-HW02	122	6800	10200	15300

Fig. 3.13 Dashboard view—annual increases of Asset's risk- tabular view

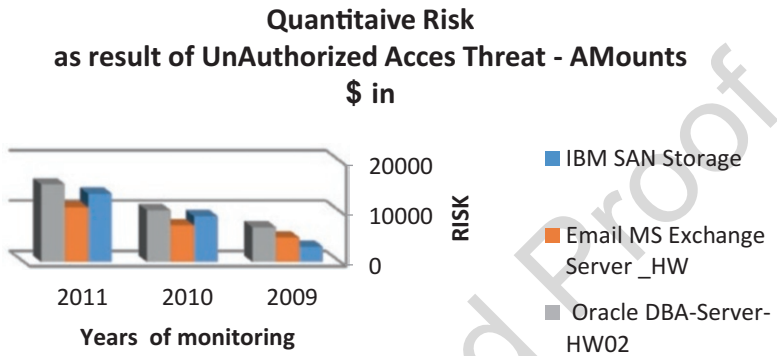


Fig. 3.14 Dashboard view—annual increases of Asset's risk- chart view

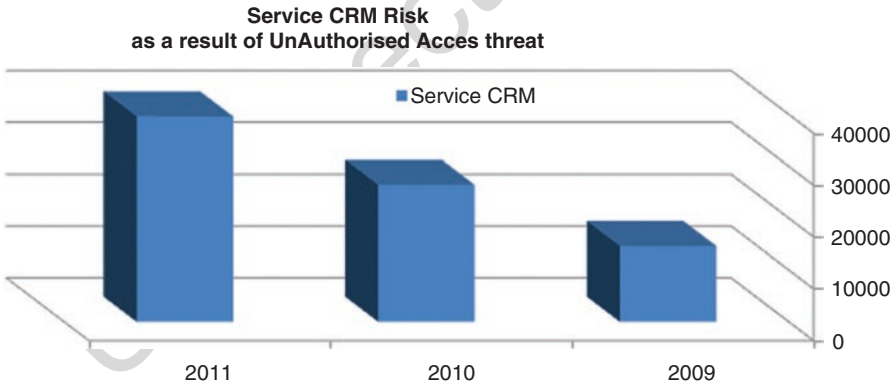


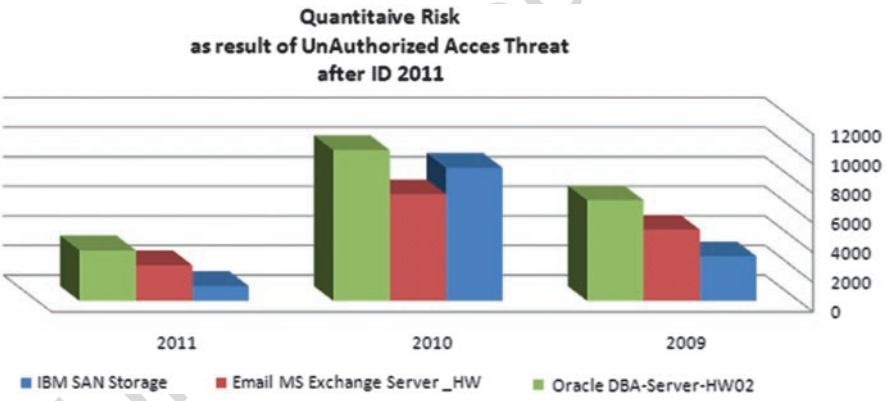
Fig. 3.15 Dashboard view—annual unauthorized access risk value –service level –chart view

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 Fig. 3.15 (Table 3.14).

Table 3.14 Scenario 3

Case 3	
Area	Risk
Name	Service level risk per threat based on historical data
Indicators	Monitoring risk level
Effective parameters	Threat assets ID and description Events year Asset value (Qltv,Qntv) Impact value (Qltv,Qntv) Risk value (Qltv,Qntv)
Searching criteria	Risk generated by threat number 25 (unauthorized access) since 2009 till 2011
Analysis and investigation	The retrieved data helps risk analysts and security specialists to determine the amount of risk generated by threat 25 since 2009, it indicates as the dashboard shows that the unauthorized access is increases on the related assets (SAN storage, email and database server).
Decision and action	An action need to be taken to protect CRM service Purchasing IPS would be a good solution providing that two out of three assets are rated HIGH (3) which considered important to be protected. Impact value is HIGH (3) for two out of three asset. As a conclusion high level asset with high level impact value is to be considered seriously.



this figure will be printed in b/w

AU5

Fig. 3.16 Dashboard view—Qltv-risk dropped in 2011 to acceptable level-chart and tabular view

Based on the 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) (Fig. 3.16).

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. 3.17).

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.

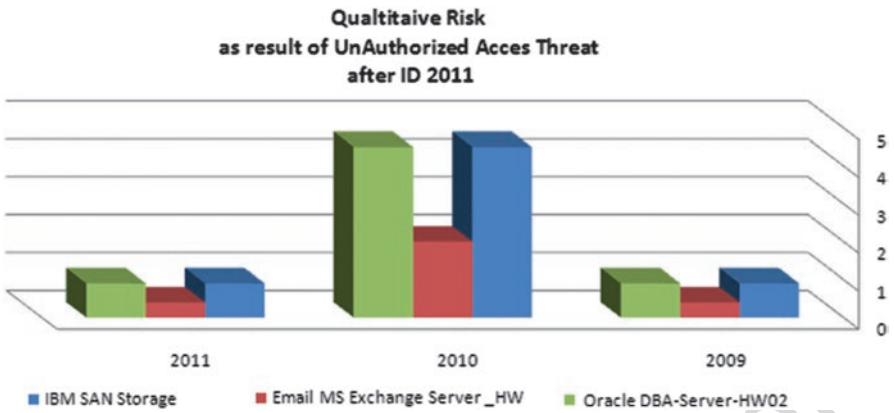


Fig. 3.17 Dashboard view—Qntv-risk dropped in 2011 to acceptable level-chart and tabular view

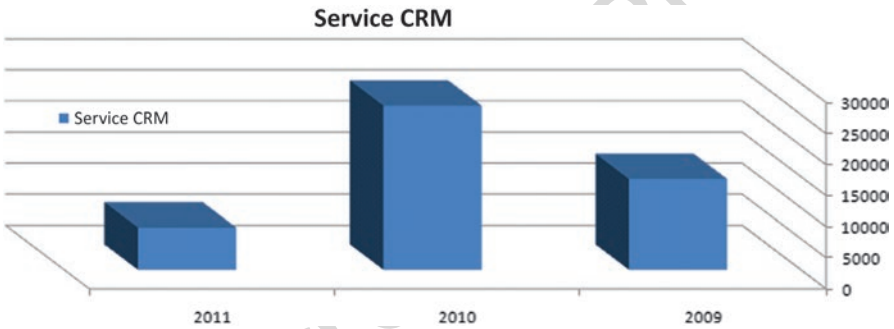


Fig. 3.18 Dashboard view—service level -risk dropped in 2011 to acceptable level-chart and tabular view

As a result CRM service Level risk is dropped to reach level less than what was in 2009 as shown in Fig. 3.18.

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 in order 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

Table 3.15 Advantage of risk database t15.1

Process	Manual and semi manual work	Proposed design
Assets information gathering/management	Using surveys, questionnaires and template forms to feed manual and automated processes	Use ITIL CMDB as reference or consider the risk database a good assets repository/ inventory which can serve and feed other systems like helpdesk and change and incident systems
Threats dependencies and handling	Generates threat statement based on: Historical data(system attacks) that is collected periodically from different systems and resources Well known attacks by vendors	A full threat's repository for the current existing threats and expected ones based on assets nature vulnerabilities. Automated display (dashboard viewer) for all possible threats, discovery details and existing and proposed controls
Risk mitigation	Qualitative OR quantitative approach. Risk evaluated at asset level only Manual or systematic way of calculation with restriction	Risk evaluation and calculation in both qualitative and quantitative approaches; gives a wide range of evaluation criteria and better understanding of risk A service/system level risk view, with drilling capability to asset level. Automated risk calculation and flexible way to change calculation parameters
Presentation layer	Manuals and hardcopy documents Complicated and very expensive systems	Dashboard viewer that reads directly from the proposed database and required no application.

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 considered to be 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. Manual work can be a hectic activity as it depends on various entities and individuals; accuracy and consistency might be an issue, collecting and filtering information requires lots of efforts and man hours. The following Table 3.15 describes the advantages of a risk database over manual activities:

Finally, a risk database is a good resource for top management to build their conclusions based on collected data and take the proper action against risks at the right time. The senior manager must decide to reduce the risk, accept the risk, or delegate the risk to someone else. A security risk can be reduced by implementing additional security controls or even by improving existing security controls (Landoll 2006).

References

Almadhoob, A., Valverde, R.: Cybercrime prevention in the Kingdom of Bahrain via IT security audit plans. J. Theor. Appl. Inf. Technol. **65**(1), 274–292 (2014)

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

Dawson, C.W.: Projects in Computing and Information Systems: A Student's Guide. Pearson Education, Harlow (2009)

DeSouza, E., Valverde, R.: An employee-based risk management strategy for reducing security incidents in a Canadian PHIPA regulated environment. In: International Conference on Innovations in Computer Science and Information Technology (ICICSIT -2015), Hyderabad (2015)

Harris, S.: CISSP All-in-One Exam Guide. McGraw-Hill Inc., New York (2008)

Khan, N.A., Valverde, R.: The use of RFID based supply chain systems in data centers for the improvement of the performance of financial institutions. Eng. Manage. Res. **3**(1), 1–24 (2014)

Kouns, J., Minoli, D.: Information Technology Risk Management in Entreprise Environments. Wiley (2010)

Landoll, D.: The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments. CRC Press, Boca Raton (2006)

Nijburg, E., Valverde, R.: A business continuity monitoring model for distributed architectures: a case study. Int. J. Appl. Sci. Technol. **1**(2), 5–14 (2011)

Stephens, J., Valverde, R.: Security of e-procurement transactions in supply chain reengineering. Comput. Inf. Sci. **6**(3), (2013)

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

Tan, D. Quantitative risk analysis step-by-step. SANS Institute (2002)

Wheeler, E.: Security Risk Management: Building an Information Security Risk Management Program from the Ground Up. Elsevier (2011)

Wolden, M., Valverde, R., Talla, M.: The effectiveness of COBIT 5 information security framework for reducing cyber attacks on supply chain management system. IFAC-PapersOnLine. **48**(3), 1846–1852 (2015)

Atif Amin is an IT manager with the Dubai Statistics Center in Dubai United Arab Emirates. Atif completed a Master of Science in Information Technology at the University of Liverpool in Liverpool England. Atif has international experience in IT from different countries and holds several certifications. Atif's main research interest include business intelligence, data centers and IT management.

Dr. Valverde is a Senior Lecture in Supply Chain and Business Technology Management at Concordia University. He holds a Doctorate in Information Systems from the University of Southern Queensland, Post MBA from McGill University, MSc in Accounting & Financial Management from the University of the West of England, Master of Logistics and Supply Chain Management from Camilos Jose Cela University, MEng in Electrical & Computer Engineering from Concordia University and a BSc in Management Mathematics and Computer Technologies from Excelsior College of the University of the State of New York. Dr. Valverde's main research interests include IT and Finance in Supply Chain, IT in Finance, Project Cost Management, Risk in IT and Supply Chain and NeuroIS.

Author Queries

Chapter No.: 3 0003183376

Queries	Details Required	Author's Response
AU1	Please confirm affiliation details for Raul Valverde.	
AU2	Citation Khan and Valverde (2013) has been changed to Khan and Valverde (2014). Please check.	
AU3	Plaese confirm inserted citation for Figs. 3.1, 3.4, 3.7, 3.9, 3.10, 3.16, 3.17 and Tables 3.1–3.5, 3.7, 3.10, 3.12, 314, 3.15.	
AU4	"asst" has been changed to "asset" here and other occurrence. Please check.	
AU5	Figures are stretched, please provide better quality artwork for Figs. 3.16–3.18.	
AU6	Please provide page range for Stephens and Valverde (2013).	
AU7	Please provide location for Stoneburner et al. (2002) and Tan (2002).	
AU8	Please provide publisher location for Kouons and Minoli (2010) and Wheeler (2011).	