# 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
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

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
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 com-
ponents, 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 rela-
   tional 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 miti-
   gate 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:

\[
\text{threats} \times \text{vulnerability} \times \text{asset value} = \text{total risk} \\
(\text{threats} \times \text{vulnerability} \times \text{asset value}) \times \text{controls gap} = \text{residual risk}
\]  

Harris (2008) also illustrates Residual Risk as:

\[
(\text{threats, vulnerability, and asset value}) = \text{total risk} \\
\text{total risk} - \text{countermeasures} = \text{residual risk}
\]

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 conceived 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>
<thead>
<tr>
<th>Table 3.1 Controls types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control type</td>
</tr>
<tr>
<td>Detective</td>
</tr>
<tr>
<td>Directive</td>
</tr>
<tr>
<td>Preventive</td>
</tr>
<tr>
<td>Corrective</td>
</tr>
<tr>
<td>Recovery</td>
</tr>
</tbody>
</table>

Controls that associated with disaster recovery and business continuity processes. | t1.7 |
|---|---|

300 301 302 303 304 305 306

307 308 309 310 311 312 313

314 315 316

317 318 319 320 321 322 323

324 325

t1.1 t1.2 t1.3 t1.4 t1.5 t1.6 t1.7 t1.8
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:
• 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 experi-
enced 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 pro-
cess 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
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 evalu-
ated by related members. The following Table 3.2 describes how assets are evalu-
ated 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 question-
naires 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
Based on best practices at Dubai Statistic Center threats data can be gathered from the following sources:

- Historical systems attacks
- World wide data
- Surveys and Questionnaires

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

### Table 3.2 Assets values based on qualitative approach/Dubai Statistic Center

<table>
<thead>
<tr>
<th>Assets values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High values assets</td>
<td>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</td>
</tr>
<tr>
<td>Medium value assets</td>
<td>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.</td>
</tr>
<tr>
<td>Low value asset</td>
<td>Loosing or staling such assets would not compromise organization’s CIA and would result in minor disruption Example printer, scanner, telephone device and others similar.</td>
</tr>
</tbody>
</table>

### Table 3.3 Other parameters effecting assets

<table>
<thead>
<tr>
<th>Asset parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assets dependency level</td>
<td>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 databases should worth more to the organization than a server with a single software that is installed on it)</td>
</tr>
<tr>
<td>Assets access level/classifications</td>
<td>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?</td>
</tr>
<tr>
<td>Asset age</td>
<td>Represent the number of years that the asset is operating.</td>
</tr>
<tr>
<td>Conclusion: in order to assign a value to asset (high, medium, and low) the above parameters are to be considered.</td>
<td></td>
</tr>
</tbody>
</table>
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 refer-
cencing 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.
Based on the previous table, impact values can be presented as following (Table 3.8):

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):

\[
\text{Risk} = \text{Asset Value} \times \text{Impact} \times \text{Likelihood of Threat} \tag{3}
\]

**Quantitative Risk Assessment Methodology**

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:

**Financial Cost:**
- Market Cost
- Development Cost (in case of Application Software)
- Installation and Configuration Value
- Maintenance and Support Cost
- Replacement Cost
- Operation and running Cost (electricity, License in case of software)
- Depreciation Cost
Non Financial Cost

- Value to organization (like Organization Reputation)
- Asset value to users and customers

Based on previous assets parameters provided, the following formula can be generated and used to set quantitative value to asset.

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

The exposure factor (EF) represents the percentage of loss a realized threat could have on a certain asset (Harris 2008; Kouns and Minoli 2010). Single Loss Expectancy (SLE) is the total amount of revenue that is lost from a single occurrence of the risk (Kouns and Minoli 2010). Annual Rate of Occurrence (ARO) is the normalized rate at which the risk exposure resulting in actual damage occurs during 1 year (Kouns and 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 as below:

\[
\text{Single Loss Expectancy (SLE)} = \text{Asset Value} \times \text{Exposure Factor (EF)}
\]
\[
\text{Annual Loss Expectancy (ALE)} = \text{SLE} \times \text{Annual Rate of Occurrence (ARO)}
\]

Data for the proposed dashboard viewer can be presented as:

- Charts
- Tables

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

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

<table>
<thead>
<tr>
<th>Case #</th>
<th>The case description or the criteria title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>How this case was explored? What are the risk indicators?</td>
</tr>
<tr>
<td>Indicators</td>
<td>What are the related parameters?</td>
</tr>
<tr>
<td>Effective parameters</td>
<td>Example asset value, impact value.</td>
</tr>
<tr>
<td>Searching criteria</td>
<td>What is the searching criteria, what to look for and where?</td>
</tr>
<tr>
<td>Analysis and investigation</td>
<td>This section covers analyzing the case (HOW?) and what indication we need to build our decision on?</td>
</tr>
<tr>
<td>Decision and action</td>
<td>Decision and action need to be taken.</td>
</tr>
</tbody>
</table>
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:

![Fig. 3.2 IT service infrastructures](image-url)
• 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.
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.
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.

Fig. 3.5 Asset information after coding

Fig. 3.6 Evaluating control template
**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.

---

**Fig. 3.7** Qualitative risk assessment

**Fig. 3.8** Quantities risk assessment
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
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). Table 3.11 presents the risk formula calculation in the risk database based on a qualitative approach.

### Table 3.10 Database tables

<table>
<thead>
<tr>
<th>Tables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td>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</td>
</tr>
<tr>
<td>Asset Information</td>
<td>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.</td>
</tr>
<tr>
<td>Assets_types</td>
<td>Assets types can be information, paper, hard copy, physical, people.</td>
</tr>
<tr>
<td>Assets_sub_types</td>
<td>Such as server, software, firewall, …</td>
</tr>
<tr>
<td>Classification Level</td>
<td>As in Table 3.1 assets access level</td>
</tr>
<tr>
<td>Threats_info</td>
<td>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.</td>
</tr>
<tr>
<td>Threats_History</td>
<td>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.</td>
</tr>
<tr>
<td>RAP_Threat_m</td>
<td>Risk assessment plan master table, which has only the final accumulative risk for all assets items after implementing controls.</td>
</tr>
<tr>
<td>RAP_Threat_D1</td>
<td>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.</td>
</tr>
<tr>
<td>RAP_Threat_D2</td>
<td>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</td>
</tr>
<tr>
<td>Threats_Controls</td>
<td>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.</td>
</tr>
<tr>
<td>Ast_access_Level</td>
<td>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.</td>
</tr>
</tbody>
</table>
Table 3.11 Qualitative risk dependencies and calculation method in the proposed database

<table>
<thead>
<tr>
<th>Risk dependency</th>
<th>Calculation method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset qualitative value AST_QLTV_VALUE</td>
<td>In qualitative approach asset is rated as (HIGH, MEDIUM, LOW) and rated as follows</td>
</tr>
<tr>
<td></td>
<td>HIGH = 3, MEDIUM = 2, LOW = 1)</td>
</tr>
<tr>
<td>Threat impact after controls are applied</td>
<td>Impact value, can be (HIGH, MEDIUM, LOW)</td>
</tr>
<tr>
<td></td>
<td>and rated as follows HIGH = 3, MEDIUM = 2, LOW = 1)</td>
</tr>
<tr>
<td>Probability of threat to occur or take place it can also be called as the likelihood of threat to occur.</td>
<td>The frequency of threat to occur</td>
</tr>
<tr>
<td></td>
<td>LOW—Occurs once every few years and rated as 0.1</td>
</tr>
<tr>
<td></td>
<td>MEDIUM- occurs once every 6 months and rated as 0.5</td>
</tr>
<tr>
<td></td>
<td>HIGH- occurs once every month and can be rated as 1</td>
</tr>
<tr>
<td>Qualitative risk (calculated value)</td>
<td>Risk is calculated in the proposed database using qualitative approach as follows:</td>
</tr>
<tr>
<td></td>
<td>RISK = ASSET value * impact value * probability of occurrence</td>
</tr>
</tbody>
</table>

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...
Table 3.12  Quantitative risk dependencies and calculation method

<table>
<thead>
<tr>
<th>Formula</th>
<th>Asset quantitative value (AST_QNTV_VALUE)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>There are many ways to measure and calculate asset qualitative value</td>
</tr>
<tr>
<td></td>
<td>Purchasing value</td>
</tr>
<tr>
<td></td>
<td>Depreciation value</td>
</tr>
<tr>
<td></td>
<td>Cost of recovery/replacement time</td>
</tr>
<tr>
<td></td>
<td>Delay and stepping time cost</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Formula</th>
<th>Single loss expectancy (calculated value)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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).</td>
</tr>
<tr>
<td></td>
<td>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$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Formula</th>
<th>Annual rate of occurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>How many time the threat can occur (usually its calculated per year)</td>
</tr>
<tr>
<td></td>
<td>Value can be between 0 to greater than one</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Formula</th>
<th>Annual loss expectancy (calculated value)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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</td>
</tr>
</tbody>
</table>

Table 3.13  Scenario 1

<table>
<thead>
<tr>
<th>Scenario # 1</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Finding high risk based on threat's impacts/qualitative approach</td>
</tr>
<tr>
<td></td>
<td>Indicators</td>
</tr>
<tr>
<td></td>
<td>Risk level (high impact and low probability), (high impact and high probability)</td>
</tr>
<tr>
<td></td>
<td>Effective parameters</td>
</tr>
<tr>
<td></td>
<td>Impact</td>
</tr>
<tr>
<td></td>
<td>Likelihood of occurrence</td>
</tr>
<tr>
<td></td>
<td>Searching criteria</td>
</tr>
<tr>
<td></td>
<td>Looking for assets or systems with:</td>
</tr>
<tr>
<td></td>
<td>High impact value and low likelihood of occurrence</td>
</tr>
<tr>
<td></td>
<td>High impact value and high likelihood of occurrence</td>
</tr>
<tr>
<td></td>
<td>Analysis and investigation</td>
</tr>
<tr>
<td></td>
<td>All high impacts values must be taken seriously; IT staff might underestimate risks with low likelihood of occurrence as they might never occur.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Decision and action</td>
</tr>
<tr>
<td></td>
<td>All high impact values are to be seriously considered even with low probability of occurrence.</td>
</tr>
<tr>
<td></td>
<td>An immediate action is to be taken for any high impact assets even if the probability of attack was very unlikely to occur.</td>
</tr>
</tbody>
</table>
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.
**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

<table>
<thead>
<tr>
<th>Case 3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Area</strong></td>
<td>Risk</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Service level risk per threat based on historical data</td>
</tr>
<tr>
<td><strong>Indicators</strong></td>
<td>Monitoring risk level</td>
</tr>
</tbody>
</table>

**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.**

---

**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.
As a result, CRM service level risk is dropped to reach a 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

<table>
<thead>
<tr>
<th>Process</th>
<th>Manual and semi manual work</th>
<th>Proposed design</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assets information gathering/management</td>
<td>Using surveys, questionnaires and template forms to feed manual and automated processes</td>
<td>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</td>
</tr>
<tr>
<td>Threats dependencies and handling</td>
<td>Generates threat statement based on: Historical data(system attacks) that is collected periodically from different systems and resources Well known attacks by vendors</td>
<td>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</td>
</tr>
<tr>
<td>Risk mitigation</td>
<td>Qualitative OR quantitative approach. Risk evaluated at asset level only Manual or systematic way of calculation with restriction</td>
<td>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</td>
</tr>
<tr>
<td>Presentation layer</td>
<td>Manuals and hardcopy documents Complicated and very expensive systems</td>
<td>Dashboard viewer that reads directly from the proposed database and required no application.</td>
</tr>
</tbody>
</table>

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


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.
<table>
<thead>
<tr>
<th>Queries</th>
<th>Details Required</th>
<th>Author’s Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>AU1</td>
<td>Please confirm affiliation details for Raul Valverde.</td>
<td></td>
</tr>
<tr>
<td>AU2</td>
<td>Citation Khan and Valverde (2013) has been changed to Khan and Valverde (2014). Please check.</td>
<td></td>
</tr>
<tr>
<td>AU3</td>
<td>Please 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.</td>
<td></td>
</tr>
<tr>
<td>AU4</td>
<td>“asst” has been changed to “asset” here and other occurrence. Please check.</td>
<td></td>
</tr>
<tr>
<td>AU5</td>
<td>Figures are stretched, please provide better quality artwork for Figs. 3.16–3.18.</td>
<td></td>
</tr>
<tr>
<td>AU6</td>
<td>Please provide page range for Stephens and Valverde (2013).</td>
<td></td>
</tr>
<tr>
<td>AU7</td>
<td>Please provide location for Stoneburner et al. (2002) and Tan (2002).</td>
<td></td>
</tr>
<tr>
<td>AU8</td>
<td>Please provide publisher location for Kouons and Minoli (2010) and Wheeler (2011).</td>
<td></td>
</tr>
</tbody>
</table>