Decision Support Systems - Risk Assessment & Asset Valuation

Prof. Ajay S. Ramteke,
Asst. Professor, Sinhgad Institutes of Business Administration & Computer Application,
Lonavala, Pune-410401. Email: ajay_ramteke@yahoo.com

ABSTRACT
A decision support system (DSS) is a computer program application that analyzes business data and presents it so that users can make business decisions more easily. It is an "informational application" (to distinguish it from an "operational application" that collects the data in the course of normal business operation). Typical information that a decision support application might gather and present would be:

- Risk Assessment
- Asset Valuation
- Decision Making-Make Decision to spend funds on security of valuable assets.

A decision support system may present information graphically and may include an expert system or artificial intelligence (AI). It may be aimed at business executives or some other group of knowledge workers.

Now a day Risk Assessment and Asset Valuation software play very important role in making proper decision to spend funds on security of valuable assets.

When you are conducting a risk assessment, it is important to define what the goals and objectives are for the risk assessment and what that organization would like to accomplish by conducting one.

Risk and vulnerability assessments provide the necessary information about an organization’s IT infrastructure and its asset’s current level of security. This level of security allows the assessor to provide recommendations for increasing or enhancing that IT asset’s level of security based on the identified and known vulnerabilities that are inherent in the IT infrastructure and its assets.

There are many best practices or approaches to consider when conducting a risk and vulnerability assessment on an IT infrastructure and its assets. These best practices or approaches will vary depending on the scope of the IT infrastructure and its assets. To properly secure and protect an organization’s IT infrastructure and assets, a significant amount of design, planning, and implementation expertise is required to ensure that the proper level of security is designed and implemented properly.

RISK ASSESSMENT BEST PRACTICES
While preparing and conducting a risk assessment, the following best practices or approaches should be considered:

- Create a Risk Assessment Policy—A risk assessment policy will define what the organization must do periodically (annually in many cases), how risk is to be addressed (for example, a minimum acceptable vulnerability window), and how that organization must carry out a risk assessment for its IT infrastructure components and its assets [1]. Creation of a risk assessment policy is usually done after the first risk assessment is conducted as a post-assessment activity. In some cases, organizations create a risk assessment policy and then implement the recommendations that the policy defines.

- Inventory and Maintain a Database of IT Infrastructure Components and IT Assets—One of the most tedious but important first steps in conducting a risk or vulnerability assessment is to identify and inventory all known IT infrastructure components and assets. Without a complete and accurate inventory of IT infrastructure components and IT assets, an asset valuation, criticality, or importance evaluation cannot be performed.
- **Define Risk Assessment Goals and Objectives in Line with Organizational Business Drivers**—Defining the risk assessment’s goals and objectives is the second step in conducting a risk assessment for your IT infrastructure components and IT assets. Aligning these goals and objectives with the organization’s business drivers will allow the organization to prioritize and focus on critical systems and assets first given the budget limitations that most organizations face.

- **Identify a Consistent Risk Assessment Methodology and Approach for Your Organization**—Defining and selecting the risk assessment methodology and approach for your organization will be dependent on the organization’s ability to identify accurate IT infrastructure components and assets, the ability to identify asset value and/or asset importance/criticality to the organization, and how the organization makes business decisions.

- **Conduct an Asset Valuation or Asset Criticality Valuation as per a Defined Standard Definition for the Organization**—Depending on the accuracy and availability of inventory documentation and asset valuation data (for example, capital dollars spent on hardware, software, integration, maintenance, staff salaries), the organization should conduct an asset valuation or asset criticality (importance) assessment to prioritize and determine which IT infrastructure components and assets are most important to the organization (either in monetary value or importance value).

- **Define and/or Limit the Scope of the Risk Assessment Accordingly by Identifying and Categorizing IT Infrastructure Components and Assets as Critical, Major, and Minor**—Depending on the scope of the risk assessment, an organization may or may not be faced with a limited budget to conduct a thorough risk and vulnerability assessment. In many cases, organizations have limited budgets to conduct a risk and vulnerability assessment and must limit the scope on the mission-critical IT infrastructure components and assets only. Although this solution exposes the organization to potential risks, threats, and vulnerabilities, a defense-in-depth approach to assessing and mitigating risks, threats, and vulnerabilities can still be pursued.

- **Understand and Evaluate the Risks, Threats, and Vulnerabilities to Those Categorized IT Infrastructure Components and Assets**—After the IT infrastructure components and assets are identified and an asset valuation or asset criticality assessment is conducted, the next step in the risk assessment and vulnerability assessment is to assess the impact that potential risks, threats, and vulnerabilities have on the identified IT infrastructure components and assets. By aligning the potential risks, threats, and vulnerabilities to the prioritized IT infrastructure components and assets, management can make sound business decisions based on the value or criticality of that IT asset and the potential risk, threats, and vulnerabilities that are known.

- **Define a Consistent Standard or Yardstick of Measurement for Securing the Organization’s Critical, Major, and Minor IT Infrastructure Components and Assets**—To properly categorize IT infrastructure components and assets, a consistent standard definition or yardstick of measurement needs to be defined. This standard definition refers to how the organization will define and categorize IT infrastructure components and assets to be Critical, Major, or Minor. This definition can be based on monetary value, requirement by law or mandate, or criticality or importance to the organization. The selection criteria or requirements for defining this standard definition should be defined by management and incorporated into the risk assessment policy when it is drafted and implemented.

- **Perform the Risk and Vulnerability Assessment as per the Defined Standard or Yardstick of Measurement for the Organization’s IT Infrastructure Assets**—After the standard definition or yardstick of measurement is defined for IT asset categorization, the risk and vulnerability assessment can be aligned to the priorities as defined by the results of the standard definition for categorization of the organization’s IT infrastructure components and assets. This is important given that most organizations have a limited budget for implementing information security countermeasures and must prioritize how they spend funds on information security, especially if they are under compliance requirements with new laws, mandates, and regulations that require them to do so or be subject to penalties.

- **Prepare a Risk and Vulnerability Assessment Final Report That Captures the Goals and Objectives Aligned with the Organization’s Business Drivers, Provides a Detailed Summary of Findings, Provides an Objective Assessment and Gap Analysis of Those Assessment Findings to the Defined Standard, and Provides Tactical and Strategic Recommendations for Mitigating Identified Weaknesses**—The risk and vulnerability assessment final report is the primary document that presents all the findings, information, assessments, and recommendations for the organization. The final assessment report becomes the instrument for management to make sound business decisions pertaining to the organization’s overall risk and vulnerability assessment and how that organization will mitigate the identified risks, threats, and vulnerabilities.

- **Prioritize, Budget, and Implement the Tactical and Strategic Recommendations Identified During the Risk and Vulnerability Assessment Analysis**—After the findings, assessment, and recommendations are presented to management, it is important to prioritize them, create a budget, and have a tactical and strategic plan for implementing the recommendations presented in
the final report. These recommendations may impact the entire organization and may take months, if not years, to fully implement. This prioritization of tactical and strategic recommendations will enable the organization to make sound business decisions with the defined goals and objectives of the risk and vulnerability assessment.

- **Implement Organizational Change Through an Ongoing Security Awareness and Security Training Campaign to Maintain a Consistent Message and Standard Definition for Securing the Organization’s IT Infrastructure and Assets**—Implementing organizational change requires an education and security awareness training plan for all employees or authorized users of the organization’s IT systems, resources, and data. Mitigating risk requires all employees and users within the organization to abide by security awareness training.

Defining and implementing these risk assessment best practices does not come easily and requires careful analysis and decision making unique to the organization’s business drivers and priorities as an organization. For example, a bank or financial institution requires more stringent use of encryption technology to ensure confidentiality of privacy data, whereas an organization that is not subject to stringent confidentiality requirements may put less investment in encryption technology and more investment in other areas. These risk assessment best practices allow an organization to consider the big picture of why that organization should conduct a risk and vulnerability assessment and how they should methodically approach the assessment. More importantly, these best practices align that organization’s business drivers and defined standards to the risk and vulnerability assessment to assist management in making sound business decisions based on available budgets, minimum acceptable vulnerability windows, and importance and criticality of IT infrastructure components and assets.

**UNDERSTANDING THE IT SECURITY PROCESS**

Foundations and Principles of Security," designing and implementing a sound IT security architecture and framework requires a thorough analysis and examination of how availability, integrity, and confidentiality (A-I-C Triad) is designed and implemented on the IT infrastructure components and assets in the overall information security plan [8].

Attacks on an IT infrastructure and assets can disrupt availability of service resulting in the following:

- **Loss of Productivity**—Downtime equals lost productivity to organizations. Lost productivity can result in loss in dollars and time.
- **Violation of Service Level Agreements**—Service providers or outsourcing service organizations can be in violation of contractual service level agreements (SLAs) that may result in penalties and financial compensation.
- **Financial Loss**—Lost productivity and violation of SLAs all result in financial loss. Depending on the criticality of the financial loss, this may change the prioritization of how that organization funds and secures its IT infrastructure components and assets.

- **Loss of Life**—System downtime or even loss of data can impact IT infrastructures and systems that are used to maintain, support, and respond to human life issues. Attacks on an IT infrastructure and assets can disrupt the integrity of information that organizations disseminate:

- **Attack against the Integrity of a System**—A system’s integrity requires sound access control processes and authentication that the user is authorized to access the system. Attacks against the integrity of the system start with access control and include the manipulation of information or data, including destruction of data.

- **Information or Data Can Be Modified, Altered, or Destroyed**—A system’s integrity can be compromised if access is granted to a perpetrator and the organization’s information or data is modified, altered, or destroyed.

**CAUTION**

Attacks on an IT infrastructure and assets can disrupt the confidentiality of information and data assets. Attacks can expose confidential information such as corporate or intellectual property secrets, financial information, and health records, which can result in identity theft. Maintaining the confidentiality of privacy records and financial data pertaining to individuals is now subject to laws, mandates, and regulations.

Unfortunately, implementing a robust IT security architecture and framework and conducting a risk and vulnerability assessment is not something that can be taken lightly by an organization. This is true given that many IT systems and applications were not designed with security in mind; many organizations are struggling to deal with the lack of security in their IT infrastructure components and applications that are currently in production. Security was always an afterthought and now for the first time, information security is in the forefront of system requirements definitions and system designs.

Security as a process would define an entire development life cycle that incorporates security requirements into the system or application design from the very beginning. By designing a system (hardware, software, or multiplatform) or application (software code) from the ground up that includes security requirements for availability, integrity, and confidentiality, minimization of the risks, threats, and vulnerabilities can be designed into the system or application up front. Security as a process would have security requirements incorporated throughout all the steps of the system or application development and design life cycle [2], [3], [4] & [5]. These steps include the following:

- **Risk/Threat/Vulnerability Analysis**—Ideally, this is done prior to any system requirements or application requirements being defined and documented. This initial risk, threat, and vulnerability analysis will attempt to identify and mitigate the exposure by incorporating
appropriate security countermeasure requirements into the overall system or application design.

- **System Requirements Definition and Design**—After a risk, threat, and vulnerability analysis is conducted, the system’s or application’s requirements definition can incorporate the technical requirements along with embedded security and security countermeasures requirements to mitigate the identified and known exposures to that system or application.

- **Functional Design**—After the system’s technical requirements definition and security requirements definition are complete, a comprehensive system or application functional design can be documented. The functional design will describe the functionality of the system or application and how security is embedded into the functionality of the system or application.

- **Security Design**—After the system requirements definition, technical design, and functional design are completed, the specific security design for the system and application can be conducted based on the security requirements that are identified as being needed. Depending on the criticality and importance of the security design, implementation of security elements into the system or application design will assist the system designers in ensuring the availability, integrity, and confidentiality of the system or application and its data.

- **System/Application Test Plan**—Like any new system or application, a thorough system or application test plan must be developed to ensure that all the technical, functional, and security design elements were developed properly and do not contain identifiable bugs, performance issues, or potential exposure to risks, threats, and vulnerabilities.

- **System Design Verification/Validation**—A thorough system design verification and validation assessment will come from the results of the system or application test plan. The results of the test plan will uncover whether the system design properly incorporated the technical, functional, and security requirements as defined in the system or application development life cycle.

This IT security process is what is currently missing from many organizations when it comes to designing and implementing new IT systems and applications throughout the organization. As organizations incorporate security requirements and design into the development life cycle, more IT systems and applications will have the inherent security controls to ensure that the availability, integrity, and confidentiality goals and objectives are achieved.

When conducting a risk and vulnerability assessment on IT systems and applications, examination of the defined security goals and objectives can be done. This examination will include a review of the IT system’s or applications’ security requirements and how they were implemented in production. Understanding this void in the development life cycle will help IT organizations fill the void with proper security requirements and security design steps in the overall development effort. By implementing the proper security controls and requirements into the system and application design up front, minimization of exposure to risks, threats, and vulnerabilities can be achieved, thus eliminating costly security countermeasures and other security controls around the IT system or application that lacks the proper security controls.

**THE GOALS AND OBJECTIVES OF A RISK ASSESSMENT**

An organization may consider many goals and objectives prior to undergoing a risk and vulnerability assessment. Some of these goals and objectives may be the result of required compliancy to new laws, mandates, and regulations for information security. Security as a process for an IT infrastructure and assets is primarily concerned with prevention, detection, and response. A sound and comprehensive security process coupled with a robust IT security architecture and framework will assist the organization in ensuring the security of the IT infrastructure and assets as per the organization’s minimum acceptable risk or exposure level.

**Security Process Definition**

Security as a process typically includes three key elements: prevention, detection, and response. Prevention deals with the implementation of security controls and countermeasures or safeguards during the initial security design phase of the development life cycle. By incorporating security requirements into the design phase of the development life cycle, prevention or protection is easier to implement because it is inherent in the system’s or application’s design up front. Prevention techniques and solutions should be designed and developed into the system or application to ensure that availability, integrity, and confidentiality for the system or application are implemented. Detection or monitoring deals with monitoring the IT infrastructure and assets. This includes monitoring log files, audit trails, intrusion detection system reporting, and reviewing vulnerability assessments reports and CVE items that are installed within the production IT infrastructure. Continuous monitoring of the IT infrastructure and assets for newly discovered risks, threats, and vulnerabilities is an ongoing process and the responsibility of information security professionals who are responsible and accountable for securing the IT infrastructure and assets.

Response is the reaction that an IT organization takes in response to a security breach or incident from a known or unknown risk, threat, or vulnerability. Response usually encompasses the following four areas:

- **Business Continuity Plan (BCP)**—Organizations that have a significant amount of investment in the IT infrastructure and assets typically create, test, and validate an internal BCP plan to address how to maintain operations and functionality in the event of lost critical assets. A BCP plan typically includes a risk assessment, asset valuation or criticality assessment, and a
vulnerability assessment in order for the organization to build the proper BCP plan in the event of risk, threat, or vulnerability incidents affecting the production IT infrastructure and assets.

- **Disaster Recovery Plan (DRP)** — Organizations that have a significant exposure to risks and threats, particularly weather related, act of God related, or war related, must have a plan for dealing with a disaster (for example, hurricane, flood, fire) [7]. A DRP plan typically requires an outsourcing solution and/or a hot site that replicates the main IT infrastructure and systems that the organization is fully dependent on to maintain its business operations.

- **Security Incident Response Team (SIRT) and Plan** — Many organizations have their own internal Security Incident Response Team (SIRT) that comprises a cross-section of human resources, legal, IT, and departmental management personnel. The SIRT typically has authority to collect and conduct investigations pertaining to security breaches and/or security incidents. Because of the potential sensitivity and nature of a security breach or incident, confidentiality and maintaining the integrity of data and information used to investigate and collect the data and information must be conducted under certain rules and guidelines. This is critical if forensic data is to be used in a court of law as evidence if a criminal charge is put on the perpetrator or perpetrators for violation of access or unauthorized use of an organization’s IT infrastructure and assets.

- **Forensic Analysis Plan** — Depending on the laws, mandates, regulations, and jurisdiction of the security breach and/or incident occurring, a carefully developed forensic analysis plan and computer forensic data and information collection must be followed for the data and information to be admissible in a court of law as evidence for a criminal case in the United States. The CIRT team must be properly trained and the IT security professionals who collect and retrieve data and information must abide by the forensic analysis plan where data and information collected during the security breach or incident investigation is pursued [6].

Depending on the organization’s compliancy requirements to new laws, mandates, and regulations, the priorities, definition of criticality or importance, and the goals and objectives that are identified for conducting a risk and vulnerability assessment will be unique to that organization.

**GOALS AND OBJECTIVES OF VULNERABILITY ASSESSMENT**

Some of the more common goals and objectives of conducting a risk and vulnerability assessment are as follows:

- IT organizations can have an accurate inventory of IT assets and data assets.
- IT organizations can have prioritized IT assets and data assets based on different measurements criteria—asset value in rupees, the importance of assets to the organization, or the criticality to the organization.
- Risks, threats, and known vulnerabilities can be identified and documented for the IT organization’s production, infrastructure, and assets.
- Risks, threats, and known vulnerabilities can be prioritized based on impact or criticality of the IT asset or data asset that it impacts.
- The vulnerability window can be identified and minimized according to the organization’s minimum acceptable tolerance to being vulnerable.
- Remediation or mitigation of the identified risks, threats, and vulnerabilities can be properly budgeted and planned according to the prioritization or criticality of IT assets and data assets.
- Compliancy with new information security laws, mandates, and regulations can be achieved by first conducting a risk and vulnerability assessment.
- Identification of the gaps or voids in the organization’s IT security architecture and framework can be found with specific recommendations for closing the gaps and voids.
- A risk and vulnerability assessment identifies the exposures, risks, threats, and vulnerabilities that the organization is subject to and assists the IT organization in justifying the cost of needed security countermeasures and solutions to mitigate the identified risks, threats, and vulnerabilities.
- A risk and vulnerability assessment provides an IT organization with an objective assessment and recommendations to the organization’s defined goals and objectives for conducting the risk and vulnerability assessment.
- A risk and vulnerability assessment assists IT organizations with understanding the return on investment if funds are invested in IT security infrastructure.

**RISK ASSESSMENT MODEL:**

Siemens Software Comprehensive Risk Assessment Tool (CRAMM) provides a staged and disciplined approach embracing both technical (eg. IT hardware and software) and non-technical (eg. physical and human) aspects of security [9]. In order to assess these components, CRAMM is divided into three stages:

1. Asset identification and valuation.
2. Threat and vulnerability assessment
3. Countermeasure selection and recommendation
PROPOSED IT SECURITY-RISK ASSESSMENT AND ASSET VALUATION MODEL

In the IT Security- Risk Assessment and Asset Valuation Model, following three steps are implemented as depicted in Figure 2.

- Risk Assessment
- Asset Valuation
- Make Decision to spend funds on security of valuable assets.

Risk Assessment Process:
In Asset Valuation and Risk Assessment Software following type of Physical & Logical assets are taken into the consideration [8].

1. Personal
2. Physical assets with IP
3. Physical assets withought IP
4. Services
5. Software
6. Documents and Information Data

Risk Assessment is carrying out based on following risk factors.

1. Threats of theft
2. National Calamities

TABLE I

<table>
<thead>
<tr>
<th>ASSET’S QUALITATIVE &amp; NUMERIC VALUES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset value (Qualitative Value)</td>
</tr>
<tr>
<td>Very High</td>
</tr>
<tr>
<td>High</td>
</tr>
<tr>
<td>Medium</td>
</tr>
<tr>
<td>Low</td>
</tr>
</tbody>
</table>

The numeric asset values as shown in the Table-I can be obtained by multiplying the ranking of Confidentiality (C), Integrity (I) and Availability (A). Risk levels are assigned to the assets based on Confidentiality, Integrity and Availability of the assets. All these three attributes have ranking from 1 to 5.

I. Very High Risk – Rank 5 – It means very high business impact in terms of financial impact.
II. High Risk - Rank 4 – It means high business impact.
IV. Low Risk – Rank 2 – It means low business or productivity impact.
V. Very Low Risk – Rank 1 - It means does not constitute to any business impact.

Confidentiality (C), Integrity (I) and Availability (A) factors can be defined as follows.

Confidentiality: Confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from jeopardizing organizations security to the disclosure of personal and confidential data resulting in contravention of privacy acts. Unauthorized, unanticipated or unintentional disclosure could result in loss of revenues, public confidence, embarrassment or legal action.

Integrity: Integrity refers to the requirements that information be protected from improper modification. Integrity is lost if Unauthorized changes are made to the data or Information.
assets by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of contaminated information could result in inaccuracy, fraud or erroneous decisions.

**Availability:** If mission critical information, software, hardware etc. assets are unavailable to its end users, the continued operation may be affected. Loss of system functionality and operational effectiveness may result in loss of productive time, thus impeding the end users performance of their function in supporting “THE COMPANY’S” mission.

Risk Assessment is performed for the particular asset using following equation (1).

\[
\text{Total Risk} = C \times I \times A
\]

**Example:**
Let us consider an example of physical assets, a personal computer (PC), Server and Logical assets, Service, Software and Data. Risk ranking applicable to Confidentiality, Integrity and Availability factors of the all these asset is shown in the following table.

<table>
<thead>
<tr>
<th>Asset</th>
<th>C</th>
<th>I</th>
<th>A</th>
<th>Total Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>125</td>
</tr>
<tr>
<td>Server</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>125</td>
</tr>
<tr>
<td>Service</td>
<td>1</td>
<td>4</td>
<td>3</td>
<td>12</td>
</tr>
<tr>
<td>Software</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>64</td>
</tr>
<tr>
<td>Data</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>100</td>
</tr>
</tbody>
</table>

Graphical representation of Assets and its risk assessment is depicted in the following Figure 3.

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Particular Loss</th>
<th>Loss or Penalty (In Rupees)</th>
<th>Remark</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Hard disk, mother board, RAM, CD-Drive stolen by intruders</td>
<td>45,000</td>
<td>Each 3 units</td>
</tr>
<tr>
<td>2.</td>
<td>Optical mouse stolen by the students</td>
<td>2,500</td>
<td>5 units</td>
</tr>
<tr>
<td>3.</td>
<td>Loss of data due to lack of security and backup system</td>
<td>5,000</td>
<td>Duration required to recover the data is approx. 30 days</td>
</tr>
<tr>
<td>4.</td>
<td>Exam forms of 60 students submitted to the university after the due date</td>
<td>60,000</td>
<td>Penalty Rs. 1000 per students.</td>
</tr>
</tbody>
</table>

| Nets Loss | 1,12,500 |

**Decision Making**
After risk assessment and asset valuation following decisions has been taken by the management to secure the valuable assets.

1. Purchased CPU security locks of Rs. 6,000
2. Installed Exam. Schedule tracking system of Rs. 5,000
3. Installed Kaspersky Anti-Virus of Rs. 48,000

In year 2007 management has Invest fund of Rs. 59,000 to secure valuable assets from risk, threats and vulnerability. Final outcome of Risk assessment and asset Valuation Decision Support System is depicted in the following figure 4.
security responsibility, segregation of duties and dissemination of these duties to IT and IT security professionals is a critical follow-up step in many IT organizations to properly address the human responsibilities and accountabilities for ensuring that the availability, integrity, and confidentiality of IT infrastructure components and assets are met. The dissemination of roles, responsibilities, and accountabilities throughout the IT infrastructure or areas of risk management can be clearly defined after the risks, threats, and vulnerabilities are identified within an organization’s IT infrastructure.

CONCLUSION
We all face risks everyday – ranging from the mundane, such as “which way shall I drive to work today?” to risks which can affect the rest of our lives, like “Shall I apply for that job?” – Risk is something we all live with and feel we practice and understand. In the information system environment, new business practices – such as outsourcing, partnership and consortiums and new technologies, such as remote working, wireless LANs and PDAs, mean that we are constantly facing new threats and risks and need for additional controls. These complexities make it practically impossible for an Information security Officers to keep up to date withouth automated support. ITSRA has for many years, been the UK Governments preferred approach to risk assessment.

- Asset Valuation and Risk Assessment System play very important role to make proper decision to spend funds on security of valuable assets.
- Because of the increase in risks, threats, and weaknesses in IT infrastructures, IT budgets must be specified to secure the IT infrastructure
- In other organizations, new laws, mandates, and regulations are requiring organizations to invest in information security and IT security infrastructure.

FUTURE SCOPE
Risk assessments allow the organization to assess from a criticality and importance factor which IT and data assets must be protected and secured more than others. In addition, a risk assessment will allow an organization to make tactical and strategic business decisions pertaining to securing its most valuable IT and data assets. Without a risk assessment, IT management would be guessing as to how best to spend its funds on security for its IT and data assets.

Finally, a risk and vulnerability assessment allows an organization to understand the roles, responsibilities, and accountabilities for the IT professionals and IT security professionals in an organization. Risk and vulnerability assessments typically find gaps and voids in the human responsibility and accountability for dealing with risks, threats, and vulnerabilities. Given the magnitude of the IT...
One can model changes to the risk assessment, using “what-if” calculations. Back-tracking can do through the risk assessment to show the justification for specific asset.

REFERENCES