Risk Assessment Models And Methodologies

JITENDER SINGH YADAV, MOHIT YADAV*, ANKIT JAIN*

Email: jitender1191m@gmail.com
      mohit12yadav@yahoo.com
      ankitjain199256@gmail.com

ABSTRACT

The fast evolution of technology and the rich capabilities of the World Wide Web have opened up bigger risks related with incorporating technology in the daily lives of individuals and organizations the entire over the world. Just as businesses are struggling to survive among competition by improving effectiveness through information technology, it is necessary to properly plan, gauge and manage the risks related with technology. "An IT risk is something that can go wrong with IT and cause a negative effect on the business". Many risk determination models or methodologies are accessible to suit different types of entities. Depending on one's size, maturity and capability, risk management models will differ. Which can help determine whether the risk appraisal and risk management activities employed by the client is commensurate and adapted. Besides independently structured IT risk methods, it is interesting to understand how company-wide risk models are tailored to compute technology risks. There are many ways to achieve valuable integrations of company-wide techniques and the appraisal of technology risks, and some of these will be explored.

KEYWORDS: Risks, Methodologies, Assessment, OCTAVE, CRAMM

1. Introduction:-

Risk calculation is the determination of quantitative or qualitative value of risk related to a concrete condition and a recognized threat. Quantitative risk computation needs calculations of two components of risk, the magnitude of the potential loss, and the probability that the loss will occur. Agreeable risk is a risk that is understood and tolerated usually because the cost or difficulty of implementing an effective countermeasure for the associated vulnerability exceeds the expectation of loss.
In every bit of types of engineering of complex systems sophisticated risk assessments are often made within Safety engineering and Reliability engineering when it concerns threats to life, environment or machine functioning. The nuclear, aerospace, oil, rail and military industries have a long history of dealing with risk appraisal. Additionally, medical, hospital, social service and food industries control risks and perform risk assessments on a continual basis. Methods for appraisal of risk may differ between industries and whether it pertains to general financial decisions or environmental, ecological, or public health risk appraisal.

All the basics of the risk management cycle are significant but risk assessment is the Headstone for all the other fundamentals. The problem of risk assessment is an really complex one. When a risk assessment process is started, this process has to analyse numerous aspects in parallel. First, we can talk about the stake at risk and how significant vulnerabilities are in the disaster situations taken into account, the result being a way to reduce the resulting risks. Second, we must understand that the chance of an event depends on a series of outside factors as well as on internal factors of the entity (business/process/project) for which the risk assessment is made. It is essential to know and control as many of these factors as possible.

2. **Qualitative vs. Quantitative:**

When risk assessment is discussed, it can be approached from two directions, two assessment models: the qualitative model and the quantitative model. The qualitative risk analysis is a process of assessment of the impact of the identified risk factors. Through this process the priorities are determined to solve the potential risk factors, depending on the impact they could have. The definite characteristic of the qualitative model is the use of subjective indexes, such as ordinal hierarchy: low-medium high, vital-critical- important, bench mark etc. Through the quantitative risk analysis it is sought to obtain some numerical results that express the probability of each risk factor and its consequences on the objectives of the project, but also the risk on the entire project level. The process uses techniques such as the Monte Carlo method for:

- determining the probability of reaching an objective;
- risk quantification on the entire project’s level and determining the additional cost that could be necessary;
- identifying proprietary risk factors through the quantification of their contribution to the risk index on the level of the entire project;
- identifying some realistic changes of cost and activity plan.

The most common formula for evaluating risk exposure is $RE = P \times L$, where:
• RE = risk exposure
• P = risk probability
• L = loss

Starting with probability of occurrence and the amount of lost (impact level) a risk Matrix can be developed in order to better understand the risk exposure.

3. Risk assessment models and methodologies:-

3.1. OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) is a self-directed methodology that enables users to gain knowledge of security problems and develop improvements to the organization’s security position without relying on external IT Specialists thus when a company has many subsidiaries around the world, where technology risks exist, it can be tailored to suit. Figure 1 provides a series of workshops during the first three phases that an organization must undergo to implement OCTAVE. This model incorporates a set of criteria involving principles, attributes, and outputs and includes the participation of company-wide employees whereby the level of importance for specific company data is determined and associated threats therein are assessed. Phase 1 involves evaluating an organization’s security strategy via employees identifying critical business assets or information that requires protection, and then summarizing the threats identified into threat profiles.

The threats considered by this model include events that cannot be controlled such as fires or floods, organizational negligence, human errors, technological errors and intentional performance of harmful activities. Phase 2 demands management to scrutinize its existing IT infrastructure components to
investigate weaknesses that open up the organization to risk exposure and vulnerabilities. Analysis is performed to assess the risks of data compromise and possible forms of attacks during Phase 3 where a risk management and mitigation plan is developed. To combat and minimize the probability of such acts from transpiring, several security measure proposed by OCTAVE can be employed, including considerations on the organization’s IT infrastructure, staff requirements, hardware and software needs, communication, and ways to prepare for unpredictable events. Concluding activities of the OCTAVE approach require top management’s approval of the protection strategy and any post-OCTAVE activities for maintaining an effective risk management plan. One advantage of using OCTAVE is that it can be adjusted to align with policies of many entities a variety of business environments.

3.2 **FAIR (Factor Analysis of Information Risk)** and its goal is to provide cost-effective information risk management through understanding, analysing, and measuring these risks. There are four stages and tens steps in the basic FAIR analysis model, and Figure 2xli depicts the major components. The first two steps in Stage 1 involves identifying the assets at risk and clearly defining whether the component of threat is human or malware (e.g. programmer/engineer and firewall program), and internal or externally. During Stage 2, the probable frequency of attacks, a quantifiable threat capability rate (e.g. “Top 2% when compared against the overall threat population”), expected effectiveness of controls and vulnerability rate (i.e. probability of asset susceptible to impact of threat) and the likelihood that the threat will cause asset damages are assessed using multiple sets of organized matrices. The forms of loss that are encompassed in a FAIR model include productivity loss, expensing of personnel time to correct deficiencies, asset replacement costs, legal/regulatory fines, compromised competitive advantage and reputational damages. Stages 3 and 4 quantify the estimated monetary loss and approximate the possibility and frequency of future losses. When estimating loss, the worse-case scenario is the absolute variable, in that individual probabilities of threat factors leading to the worse-case scenario are multiplied to find the product that would equal the likelihood of the occurrence of the worse-case scenario. For example, if a malfunctioning firewall program (probability of occurrence = 10%) and the bypassing of password authorization (probability of occurrence = 15%) are the two factors required for hackers to steal all the money from an organization’s bank account, the worse-case scenario that money would be stolen would have a probability of 10% x 15% = 1.5%. The probability of 1.5% would then be multiplied against the estimated quantifiable monetary loss to obtain the final loss estimation. Critical organizational factors that can have detrimental consequences would undergo this formula, and the aggregate monetary loss estimation would be summed to identify the magnitude and frequency of loss. Overall company risk profile will therefore be created to assess where resources are most needed to protect company assets. This method is a much more comprehensive approach to assessing and quantifying the potential risks since a significant amount of time and resources may be expended compared
to OCTAVE. Hence, it is most suitable for entities with high asset values where any losses will cause significant damages to the organization (e.g. banks).

3.3 **CRAMM (CCTA Risk Analysis and Management Method)** is a risk assessment software that first requires the IT team to identify all the physical, software, data and location assets in an information system, then value them based on replacement cost for the physical assets and the consequential impact of unavailable, damaged, or leaked information for data and software assets. The software encompasses a wide range of intentional and accidental threats to the information system such as hacking, viruses, errors, and equipment and software failures by assessing the degree of the associated risks. CRAMM software compares the measures of risks identified during the threat assessment stage against a security benchmark in order to determine whether the risks are significant enough to justify the implementation of a counter measure. From Figure 3ii, it can be seen that there are two distinct stages- analysis and management- to ensure that the implementation does not take place until a thorough analysis is complete, avoiding cost-overruns and inefficient resource allocations. There are two different versions of the CRAMM software available to assess threats and vulnerabilities, and they are CRAMM Express and CRAMM Expert. The Express version provides holistic yet basic level risk assessment tools that are typically preferred by new IT project or system managers who are branching off their IT security reliance from external information security experts. The Expert version is marketed to organizations performing comprehensive risk analyses, including various compliance regulations and global certification programmes and it includes the high-level risk assessment tools available in the express version. The CRAMM software is utilized by over 500 different users including IBM and Royal Air Force.
3.4 FIRM (Fundamental Information Risk Management) is a scorecard-based approach that requires each business unit of an enterprise to critically evaluate its business resources or assets based on 5 elements of risk, which include criticality, vulnerability, special circumstances affecting the assets, level of threat, and the possible business impact of a breach or denial-of-service. The project management leader will then collect and combine each division’s data to provide a high-level view of the risk position of the company based on the risk exposure of the identified assets. The objective of this exercise is to acknowledge the overall organizational impact in the event that one or more of these assets are negatively affected by threats. Since the scorecards are jointly mapped in a visual manner, data that has been entered and collected is easily identifiable by the reader and areas requiring additional analysis can be pointed out clearly.

3.5 FRAAP (Facilitated Risk Analysis and Assessment Process) involves analysing systems, applications, platforms, business processes, or segments of business operations on an individual basis, relying on an organization’s own personnel to conduct the risk assessment process. There are three distinct FRAAP phases, which are pre-FRAAP, FRAAP session, and post-FRAAP, and the process is conducted by a trained facilitator who leads the organization through threat identification, assessment and selection of potential controls. The main focus is on the FRAAP session stage as it is then that potential threats to the integrity, confidentiality, and availability of information resources are identified. Based on the threat probability, members of the session will prioritize threats and their related impact on the operations of the business. Quantitative estimates are generally not used in a FRAAP unless the relevant data is easily obtainable. Rather, publications on threats and vulnerabilities obtained from national incident response centres, professional associations and literature and the team’s personal experiences form a part of the analysis of the likelihood and cost of threats. Controls that could be applied to reduce the risk will be identified, emphasizing on the most cost-effective controls that can cover and address a wide variety of threats. The FRAAP session demands no more than simple tools such as flip charts, colour pens, tent cards and push pins and approximately four hours of employee time. Consequently organizations that implement FRAAP
believe that risk assessment should be an economical process and specific loss estimates are not required to determine if a control is needed. Post-FRAAP activities include analysing results and preparing a summary report to be reviewed by management, which normally take less than five days. As a result, members of the team must be highly knowledgeable and familiar with the company’s IT structure and best practices, given the heavy reliance on the expertise of the project members when identifying risks and risk management recommendations.

4. Future Aspects:-

The basics presented before do, in truth, perform a risk assessment, but more through risk the external incident with devastating potential, the financial costs it causes etc. For this reason, we think that other fundamentals can also be measured in risk assessment, such as:

- The professionalism of the assessment team / trust granted to the human factor
- The time available to make the assessment
- The moment of risk identification in the system’s life cycle (analysis, project, Implementing, testing, effective functioning etc.)
- The necessary cost for assessment and adopting the risk response plan – acceptance, avoidance or transfer. (“Is the assessment still worth if it generates a cost higher than the damage that would be generated in the case of a risk occurrence?”);
- The STEEP factors (social, technological, economic, environmental and political).

5. Conclusion :-

In our opinion all the elements mentioned above are important but, as presented in the paper, we propose another extension: the human factor (considering all the aspects related to it professionalism, skills and abilities, psychological factors), the most uncontrollable part of every system. If all these elements are evaluated starting from a high-medium-low type criteria, the assessment will be qualitative. To the degree to which each of these elements is quantified into independent objective indexes such as the monetary value of replacing the value of the asset or the annual occurrence rate for the frequency of the threat, risk assessment becomes predominantly quantitative. If all the six elements we have mentioned above (including the psychological factors we have referred to) are quantified through objective independent indexes, risk assessment is fully quantitative, undergoing a series of statistical analyses.

References :-

JITENDER SINGH YADAV  et al. IJSRE et al. vol 1 issue 6 OCT 2013