UNDERSTANDING ENTERPRISE RISK MANAGEMENT AND FAIR MODEL WITH THE HELP OF A CASE STUDY

Adesh Chandra, Anurag Singh & Ishan Rastogi
(Department of M.S.-CLIS, IIIT Allahabad, India)

ABSTRACT

Risk is the probability of suffering a loss, destruction, modification or denial of availability of an asset. Enterprise risk management includes the various processes to manage risk and helps to provide a framework to analyze and determine risks. There are various framework to analyze risk but here we will study about FAIR (Factor analysis of information risk). FAIR derives risk on the basis of certain parameters which help in the estimation of probable loss to the company. We have also taken a case study which is solved with the help of FAIR model, which will increase the understanding about enterprise risk and its various factors.

Keywords- FAIR, Threat, Vulnerability, Risk, Loss

1. INTRODUCTION

Enterprise Risk can include a variety of factors with potential impact on organizations activities, processes and resources. External factor may result economic change, financial market developments and danger arising in political, legal, technological and demographic environments. Risks can arise over time, as the public can may change their views on products or practices. Risk can be in form of probable loss to the enterprise, non-completion of goal on stipulated time and many more.

Enterprise risk management (ERM) in business includes the methods and processes used by organizations to manage risks and seize opportunities related to the achievement of their objectives. ERM provides a framework for risk management, which typically involves identifying particular events or circumstances relevant to the organization's objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring progress. By identifying and proactively addressing risks and opportunities, business enterprises protect and create value for their stakeholders, including owners, employees, customers, regulators, and society overall.

Managing risks in project is imperative for its success. We need to have processes in place for risk management to be effective. Here are the five steps which can be used for risk management:
FAIR (Factor Analysis of Information Risk) which is a widely adopted framework for risk identifying, analyzing, building and analyzing risk. FAIR defines six kind of loss: 

1. Productivity – a reduction of the organization to effectively produce goods or services in order to generate value

There are various important ERM frameworks, each of which describes an approach for identifying, analyzing, responding to, and monitoring risks and opportunities, within the internal and external environment facing the enterprise. Management selects a risk response strategy for specific risks identified and analyzed.[1] We will try to analyze FAIR (Factor Analysis of Information Risk) which is a widely adopted framework for risk management.

2. FACTOR ANALYSIS OF INFORMATION RISK

Factor analysis of information risk (FAIR) is a taxonomy of the factors that contribute to risk and how they affect each other. It is primarily concerned with establishing accurate probabilities for the frequency and magnitude of loss events. FAIR provides a reasoned and logical framework for answering following questions:

• A taxonomy of the factors that make up information risk. This helps us to have a foundation understanding of information risk.
• A method of measuring the factors that drive information risk.
• A Computational engine that drives risk by mathematically simulating the relationship between measured factors.
• A simulation model that allows us to apply the taxonomy, measurement model and computational engine to build and analyze risk.

FAIR defines six kind of loss:

1. Productivity – a reduction of the organization to effectively produce goods or services in order to generate value
2. Response – the resources spent while acting following an adverse event
3. Replacement – the expense to substitute/repair an affected asset
4. Fines and judgments (F/J) – the cost of the overall legal procedure deriving from the adverse event
5. Competitive advantage (CA) - missed opportunities due to the security incident
6. Reputation – missed opportunities or sales due to the diminishing corporate image following the event

FAIR defines value/liability as:
1. Criticality – the impact on the organization productivity
2. Cost – the bare cost of the asset, the cost of replacing a compromised asset
3. Sensitivity – the cost associated to the disclosure of the information, further divided into:
   a) Embarrassment – the disclosure states the inappropriate behavior of the management of the company
   b) Competitive advantage – the loss of competitive advantage tied to the disclosure
   c) Legal/regulatory – the cost associated with the possible law violations
   d) General – other losses tied to the sensitivity of data

FAIR characterizes risk on the basis of two parameters:
- The magnitude (severity) of possible adverse consequences
- The likelihood (probability) of occurrence of each consequence

Risk is a probability issue. Risk has both frequency and the magnitude component which forms the basis of FAIR model and helps to analyze future loss. The frequency and magnitude namely Loss event frequency and probable loss magnitude respectively are further divided on other factor for a better analysis.

2.1 Loss event frequency is the probable frequency, within a given timeframe, that a threat agent will inflict harm upon an asset. Loss event frequency is further divided into Threat Event frequency and Vulnerability.

   2.1.1 Threat event frequency is the probable frequency, within a given timeframe, that a threat agent will act against an asset. It also depends on Contact frequency and Probability of Action.

   a) Contact frequency is the probable frequency, within a given timeframe, that a threat agent will come into contact with an asset. Contact can be random, regular or intentional.
b) **Probability of action** is the probability that a threat agent will act against an asset once contact occurs.

### 2.1.2 Vulnerability

Vulnerability is the probability that an asset will be unable to resist the actions of a threat agent. It also depends on Threat capability and Control strength.

a) **Threat capability** is the probable level of force that a threat agent is capable of applying against an asset.

b) **Control strength** is the strength of a control as compared to the minimum threshold level.

---

**Figure 3 Components of Loss event frequency**

### 2.2 Probable loss magnitude

Probable loss magnitude defines various types of losses like productivity, response, replacement, fines and judgement, competitive advantage and loss to reputation. For better understanding Probable loss magnitude is further divided into Primary factors and Secondary factors.

#### 2.2.1 Primary Factors

Primary Factors comprises of the assets and the threats which the assets can have.

#### 2.2.1.1 Asset Loss Factor

There are two asset loss factors that we are concerned with which are value/liability and volume. The value/liability characteristics of an asset play a key role in both the nature and magnitude of loss. We can further define value/liability as:

1. **Criticality** – characteristics of an asset that have to do with the impact to an organization’s productivity. For example, the impact a corrupted database would have on the organization’s ability to generate revenue
2. **Cost** – refers to the intrinsic value of the asset – i.e., the cost associated with replacing it if it’s been made unavailable (e.g., stolen, destroyed, etc.). Examples include the cost of replacing a stolen laptop or rebuilding a bombed-out building
3. **Sensitivity** – the harm that can occur from unintended disclosure. Sensitivity is further broken down into four sub-categories:
   a) Embarrassment/reputation – the information provides evidence of incompetent, criminal, or unethical management. Note that this refers to reputation damage resulting from the nature of the information itself, as opposed to reputation damage that may result when a loss event takes place.
   b) Competitive advantage – the information provides competitive advantage (e.g., key strategies, trade secrets, etc.). Of the sensitivity categories, this is the only one where the sensitivity represents value. In all other cases, sensitivity represents liability.
   c) Legal/regulatory – the organization is bound by law to protect the information
   d) General – sensitive information that doesn’t fall into any of the above categories, but would result in some form of loss if disclosed.

Asset volume simply recognizes that how many assets are at risk to greater loss magnitude if an event occurs – e.g., two children on a rope swing versus one child, or one sensitive customer record versus a thousand.[3]
2.2.1.2 Threat loss factor considers on three loss factors action, competence and whether that the threat agent is internal or external.
   1. Action - Threat agents can take one or more of the following actions against an asset:
      a) Access – simple unauthorized access
      b) Misuse – unauthorized use of assets (e.g., identity theft, etc.)
      c) Disclose – the threat agent illicitly discloses sensitive information
      d) Modify – unauthorized changes to an asset
      e) Deny access – includes destruction, theft of a non-data asset, etc.
   2. Threat competence - It is the amount of damage a threat agent is able to inflict.
   3. Threat agent can be internal or external.

2.2.2 Secondary factors are those organizational and external characteristics of the environment that influence the nature and degree of loss.

2.2.2.1 Organisational factors - There are many organizational loss factors. But, we will focus on timing, due diligence, response, and detection.

   1. Timing- The timing of an event can have a tremendous impact on loss.
   2. Due diligence - It deals with the legal aspects involved in the enterprise.
   3. Response- It’s how well the organization response to the threats. There are three components to response:
      a.) Containment – It has to do with an organization’s ability to limit the breadth and depth of an event – for example, cordon-off the network to contain the spread of a worm
b.) Remediation – It has to do with an organization’s ability to remove the threat agent – e.g., eradicating the worm
c.) Recovery – It refers to the ability to bring things back to normal

4. Detection- It is how soon a threat can be detected.

2.2.2.2 External Factors- Other external factors are legal and regulatory issues, competitors of the organization, media, detection of threat and stakeholders.

3. BENEFITS OF FAIR MODEL

• Helps us to better understand our problem space. We can better analyze the problem on the basis of the parameter involved.
• Promotes thorough and consistent analyses
• Provides a framework for metrics and data analysis
• Increases credibility with stake-holders
• Improves communication within the profession and with stake-holders
• Promotes well-informed decision-making

4. HOW FAIR MEASURES RISK FACTORS

FAIR defines that risk can be determined by loss event frequency and probable loss magnitude. So here we will see that how we can determine these two factors. Loss event frequency depends on threat event frequency and vulnerability.

Measuring Threat event frequency- We can create a table with our own scale on which we can rate the frequency of a threat. The scale can comprise of very high, high, moderate, low and very low. The table can be as follows:
Rating | Description
---|---
Very High (VH) | Greater than 100 times per year
High (H) | Between 10 and 100 times per year
Moderate (M) | Between 1 and 10 times per year
Low (L) | Between .1 and 1 times per year
Very Low (VL) | Less than 1 times per year

Table 1. Table for rating Threat event frequency

Measuring Threat capability - We can create a table with our own scale on which we can measure the capability of threat that how harmful it can be as compared with all other possible threats. The scale can comprise of very high, high, moderate, low and very low. The table can be as follows:

Rating | Description
---|---
Very High (VH) | Top 2% when compared against all the possible threat.
High (H) | Top 16% when compared against all the possible threat.
Moderate (M) | Average skill and resources (between bottom 16% and top 16%)
Low (L) | Bottom 16% when compared against all the possible threat.
Very Low (VL) | Bottom 2% when compared against all the possible threat.

Table 2. Table for rating Threat capability

Measuring Control strength - The strength of any preventative control has to be measured against a baseline level of force. Till now no well-established scale exists. We can create a table with our own scale on which we can measure the control strength of various preventive measures that how much they are effective in preventive possible threats. The scale can comprise of very high, high, moderate, low and very low. The table can be as follows:

Rating | Description
---|---
Very High (VH) | Protects against all but not against the top 2% of threat population
High (H) | Protects against all but not against the top 16% of threat population
Moderate (M) | Protects against the average threat agent
Low (L) | Only protects against bottom 16% of an avg. threat population
Very Low (VL) | Only protects against bottom 2% of an avg. threat population

Table 3. Table for rating Control strength

Deriving Vulnerability - As vulnerability is a factor of threat capability and control strength which we have already measured. So we can easily make a matrix with one parameter as threat capability and other as control strength which will define the vulnerability as very high, high, moderate, low and very low. Where the threat capability and control strength intersect that determine the level of vulnerability. The matrix can be as follows:

[Figure 8 Matrix for deriving vulnerability]
Deriving Loss event frequency - As now vulnerability is been derived and earlier we have measured threat event frequency. So now we can make a matrix with these two factors as parameter. Loss event frequency is defined at the point where these two intersect. The matrix can be as follows:

![Matrix for deriving loss event frequency](image)

Measuring probable loss magnitude - We can rate probable loss magnitude on the scale of severe, high, significant, moderate, low and very low depending on the value of possible loss in terms of money a probable threat can be to the enterprise. It can be determined with the help of a table below:

<table>
<thead>
<tr>
<th>MAGNITUDE</th>
<th>RANGE FROM in Rs.</th>
<th>RANGE TO in Rs.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severe (SV)</td>
<td>1,00,00,000</td>
<td>---</td>
</tr>
<tr>
<td>High (H)</td>
<td>10,00,000</td>
<td>9999999</td>
</tr>
<tr>
<td>Significant (SG)</td>
<td>1,00,000</td>
<td>999999</td>
</tr>
<tr>
<td>Moderate (M)</td>
<td>10,000</td>
<td>99999</td>
</tr>
<tr>
<td>Low (L)</td>
<td>1000</td>
<td>9999</td>
</tr>
<tr>
<td>Very Low (VL)</td>
<td>0</td>
<td>999</td>
</tr>
</tbody>
</table>

Table 4 Table for determining magnitude of probable loss

Estimating risk - As now loss event frequency and probable loss magnitude both are known. So we can determine the risk by making a matrix based on these two parameter and the intersection of these two parameter will yield the probable risk. The risk can be rated as high, moderate, low and critical. The matrix can be as follows:

![Matrix for determining level of risk](image)
5. CASE STUDY

Scenario- An organization which deals with huge amount of data has a database server, but does not have an alternative database server which is soon to get implemented in the company after a couple of days. The company suddenly faces a database server crash down due to which the company can no more access its data and is facing loss until the server is restored to normal condition.

The analysis

As earlier we have studied about FAIR model and its steps. So we will use the same steps to derive the level of risk in this scenario.

Stage 1 – Identify scenario components
- Identify the asset at risk
- Identify the threat community under consideration

Stage 2 – Evaluate Loss Event Frequency (LEF)
- Estimate the probable Threat Event Frequency (TEF)
- Estimate the Threat Capability (TCap)
- Estimate Control strength (CS)
- Derive Vulnerability (Vuln)
- Derive Loss Event Frequency (LEF)

Stage 3 – Evaluate Probable Loss Magnitude (PLM)
- Estimate worst-case loss
- Estimate probable loss

Stage 4 – Derive and articulate Risk
- Derive and articulate Risk [4]

Stage 1-Identify scenario components

Step 1-Identify the assets at risk
The primary asset at risk is the database server which is not working, then the data contained in the database, all the applications, files and other resources which are accessed with the help of database server. In short the whole working is hampered just because of the database server.

Step 2- Identify the threat community
Now the next step is to identify whether the threat agent is human or malware, and internal or external. In this scenario the probable threat agent could be:
- Any disgruntle employee
- Any malicious software/virus
- Disk failure
- Physical damage
- Sudden power failure

With experience it become easier to determine which threat agent are responsible for the damage. In this example we are focusing on any malicious software which could be the probable cause to the damage caused.

Stage 2 – Evaluate Loss Event Frequency (LEF)

Step 1- Estimate the probable Threat Event Frequency (TEF)
TEF estimate would be based upon how frequently contact between this threat agent (the malicious software) and the database server occurs AND the probability that they would act against the database server. Recognizing that there are many malicious software which always try to get access but the frequency that any malicious software would gain access over the database is very low because the database is always being protected by antivirus, software and technical staff. So we can rate TEF on the basis of the table below:
Step 2- Estimate the Threat Capability (TCap)
TCap refers to the threat agent’s skill and resources that can be brought to bear against the asset. It refers to the capability of threat. In this scenario, the malicious capability can cause great harm to the database server. It might disclose the data to the hacker or it can simply deny access. So the threat capability is very high as it can cause more harm as compared to other probable threats. The table below will help to determine TCap as follows:

<table>
<thead>
<tr>
<th>Rating</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High (VH)</td>
<td>Top 2% when compared against all the possible threat.</td>
</tr>
<tr>
<td>High (H)</td>
<td>Top 16% when compared against all the possible threat.</td>
</tr>
<tr>
<td>Moderate (M)</td>
<td>Average skill and resources (between bottom 16% and top 16%)</td>
</tr>
<tr>
<td>Low (L)</td>
<td>Bottom 16% when compared against all the possible threat.</td>
</tr>
<tr>
<td>Very Low (VL)</td>
<td>Bottom 2% when compared against all the possible threat.</td>
</tr>
</tbody>
</table>

Table 6 Table for rating Threat capability

Step 3- Estimate Control strength (CS)
Control strength has to do with an asset’s ability to resist compromise. In our scenario, the database server is compromised, generally, database are protected to be against these type of attack. But this could be a new virus or malicious software which have crashed the database server. Usually, the control strength of database server is high, which can be determined by the table below:

<table>
<thead>
<tr>
<th>Rating</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High (VH)</td>
<td>Protects against all but not against the top 2% of threat population</td>
</tr>
<tr>
<td>High (H)</td>
<td>Protects against all but not against the top 16% of threat population</td>
</tr>
<tr>
<td>Moderate (M)</td>
<td>Protects against the average threat agent</td>
</tr>
<tr>
<td>Low (L)</td>
<td>Only protects against bottom 16% of an avg. threat population</td>
</tr>
<tr>
<td>Very Low (VL)</td>
<td>Only protects against bottom 2% of an avg. threat population</td>
</tr>
</tbody>
</table>

Table 7 Table for rating control strength

Step 4-Derive vulnerability
As we have determined threat capability and control strength. So it’s now easy to derive vulnerability by the help of a matrix with TCap and control strength as its parameter and the intersection point yields the vulnerability. In this scenario, the vulnerability is high which can be seen as follows:

Figure 11 Matrix for deriving vulnerability
Step 5 - Derive loss event frequency
Loss event frequency by intersecting threat event frequency and vulnerability which is very low for our scenario, it can be seen with help of the matrix below:

![Matrix for deriving loss event frequency](image)

Stage 3 – Evaluate Probable Loss Magnitude (PLM)
In our scenario the database is not working and that is because of malicious software which hampers the productivity, reputation and may lead to competitive advantage to other companies. The database server crash down has affected all the processes of the company.

Step 1 - Estimate worst-case loss
Here we will try to analyze the various types of loss which the company would face. Within this scenario, three potential threat actions stand out as having significant loss potential – misuse, deny access and disclosure.

- Misuse - If the malicious software is still being controlled by the hacker and is providing access to the hacker than the data could be misused which introduces potential legal and reputational loss. However in these types of cases the server is isolated at once and is looked out by the technical staff.
- Deny access - The database server is a necessary part of operating company processes. Consequently, the denial of access of server can introduce large degree of loss in productivity, competitive advantage to other companies and loss in reputation.
- Disclosure - Employee records, data about clients and many more, database often have sensitive personal information and other related data which are necessary for daily processes whose disclosure may lead to legal and reputational loss.

In many cases it’s necessary to evaluate the loss associated with more than one threat action in order to decide which one has the most significant loss potential. In our scenario, we’ll select deny access as our worst-case threat action because if the database is not working and its access is denied for a single moment then the company faces huge amount of loss.

Step 2 - Estimate probable loss
In our scenario we have already opted deny access as the worst case loss. So our next step is to estimate the worst-case loss magnitude for each loss form.

<table>
<thead>
<tr>
<th>Threat Actions</th>
<th>Productivity</th>
<th>Response</th>
<th>Replacement</th>
<th>Fines/Judgments</th>
<th>Comp. Advantage</th>
<th>Reputation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Misuse</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disclosure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deny Access</td>
<td>Severe</td>
<td>High</td>
<td>---</td>
<td>Severe</td>
<td>High</td>
<td>Severe</td>
</tr>
<tr>
<td>Modification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 8 Table for probable loss by action of threat
Our estimates are based on the following reasons:

- Productivity: It’s conceivable that productivity losses could be severe as no process takes place due to the database failure.
- Response: Legal expenses associated with inside and outside legal counsel could be high, particularly if class action lawsuits were filed. Huge amount of employee, client data and critical data is at stake.
- Fines/Judgments: If the disclosed information regarding client’s personal data or company’s critical issues is compromised, then legal judgments in behalf of affected clients could be severe, particularly if a large number of clients were affected. If the information included evidence of criminal activity or incompetence on the part of management, then legal and regulatory fines and sanctions could be severe.
- Competitive advantage: If the disclosed information provided evidence of incompetence or criminal activity, competitors could, in theory, leverage that to gain advantage. Since the company is not processing due to database failure, so competitor can gain advantage which could be high.
- Reputation: If the problem is not resolved rapidly, due diligence was seriously absent, legal actions were large enough, and media response was negative and pervasive, then reputational loss associated with customer flight and stock value could be severe.

So in all we can see that denial of access result in severe magnitude of loss to the company.

Stage 4 – Derive and articulate Risk

As we have already estimated threat event frequency and probable loss magnitude. So it is very easy to determine risk. The risk can be rated as high, moderate, low and critical. In our scenario the risk associated is high which can be seen from the table below:

![Figure 13 Matrix for deriving risk](image)

6. CONCLUSION

Enterprise risk management is the comprehensive process of identification, analysis and either acceptance or mitigation of uncertainty in decision-making. Risk management is a central part of any organization’s strategic management. The focus of good risk management is the identification and treatment of these risks. As we know that risk is the factor of probability and severity associated with a threat. The paper discusses about FAIR (Factor Analysis of Information Risk) which is a model for analysis risk. FAIR determines risk as the factor of threat event frequency and probable loss magnitude of the threat. The paper also tells about the benefits of FAIR and the various steps which are taken to derive risk from the various associated threat to the enterprise. The case study taken here is also resolved with the help of FAIR and its steps which help to determine the level of enterprise risk management.

REFERENCES