INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 4 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

A CRITICAL ANALYSIS ON RISK MANAGEMENT IN GENERAL AND LIFE INSURANCE

AUTHORS - G.RAMYA* & MS. T. VAISHALI**, LLM SCHOLAR* & ASSISTANT PROFESSOR OF LAW** AT THE TAMILNADU DR. AMBEDKAR LAW UNIVERSITY (SOEL), CHENNAI

BEST CITATION – G.RAMYA & MS. T. VAISHALI, A CRITICAL ANALYSIS ON RISK MANAGEMENT IN GENERAL AND LIFE INSURANCE, INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 4 (4) OF 2024, PG. 916-920, APIS – 3920 – 0001 & ISSN – 2583-2344.

ABSTRACT

This paper starts with an introduction with a critical analysis on risk management in general and life insurance. Risk management is a systematic process for identifying, assessing, and controlling potential threats to a business or investment. It's important for insurance companies because they take on risk from their customers, and the level of risk determines the insurance premium.

Here are some key aspects of risk management:

Risk assessment

In insurance, actuaries and underwriters use risk assessment to evaluate the probability of loss and determine the premium amount.

Risk control

A plan-based strategy that aims to identify, assess, and prepare for potential hazards and disasters. Risk control methods include avoidance, loss reduction, and loss prevention.

Risk management framework

Includes the following components:

- Risk identification
- Risk measurement
- Risk mitigation
- Risk reporting and monitoring
- Risk governance

Compliance risk

The legal, financial, and criminal exposure a business faces if it doesn't follow industry laws and regulations.

Strategic risk

Any damage or loss to reputation that could prevent a business from reaching its goals.

Introduction

Risk Management has been gaining monumental importance, especially over the last few years, globally. Apart from the conventional areas that one has in mind with regard to risk management, there is just no end to the challenges that emerge afresh from hitherto unknown areas. It is this dynamic nature of business that puts an additional onus on risk management being thoroughly comprehensive. The corporate world has been gearing itself up for these new challenges; and their risk management strategies have been demonstrating the adoption of a wider coverage of business activity. As a natural consequence, the risk management strategies of insurers would also need to take a fresh look at how they are geared up for eventualities. There are various types of risks involved in life insurance which are discussed later; however the study focuses on fraud risk. Instances of life insurance fraud are increasing since few years and therefore there is a need to curtail life insurance fraud.

Risk assessment

Risk assessment is the process in which the insurance companies evaluate the risk to cover any individual. In this process,

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 4 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

various data points and possible risks to the policyholder are taken into account to determine the insurance premium. Risk assessment is done for every individual that applies for an insurance policy. Insurance companies assess risk by analysing the proposal form duly filled and submitted by the proposer. The coverage, terms and conditions will be based on the risk assessment. Only after this, a premium is quoted.

One must fill in the factual information to avoid rejection of a proposal after risk assessment. Buying an insurance policy earlier in life is always beneficial as the risk associated, or probability of loss with young individuals, is less. Apart from the proposal form, under risk assessment, insurers also consider past insurance records, claim history, sum assured, etc.

Example:

Arnab, aged 40, applied for a term life insurance policy. He filled out the proposal form and mentioned the details correctly. The insurance company conducted a risk assessment before quoting. The medical test of the risk assessment concluded that Arnab has borderline diabetes and a family history of cancer. So, covering the life of Arnab has a higher risk for the insurer as compared to a healthy 25-year young guy. Arnab had requested life insurance quotations from multiple insurance companies. The risk assessment of every insurer led to the solution that Arnab has to pay a higher premium than the ordinary case to avail of the life cover. As he was in need of a life insurance policy, he chose to pay a higher premium to get the policy from the most suitable insurance company.

Risk control

Risk control is the set of methods by which firms evaluate potential losses and take action to reduce or eliminate such threats . Risk control is the set of methods by which firms evaluate potential losses and take action to reduce or eliminate such threats. It is a technique that utilizes findings from risk assessments, which involve identifying potential risk factors in a company's operations, such as technical and non-technical aspects of the business, financial policies and other issues that may affect the well-being of the firm. Avoidance is the best method of loss control. For example, after discovering that a chemical used in manufacturing a company's goods is dangerous for the workers, a factory owner finds a safe substitute chemical to protect the workers' health. Avoidance, however, is not always possible. Loss prevention accepts a risk but attempts to minimize the loss rather than eliminate it. For example, inventory stored in a warehouse is susceptible to theft. Since there is no way to avoid it, a loss prevention program is put in place. The program includes patrolling security guards, video cameras and secured storage facilities. Insurance is another example of risk prevention that is outsourced to a third party by contractLoss reduction accepts the risk and seeks to limit losses when a threat occurs. For example, a company storing flammable material in a warehouse installs state-of-the-art water sprinklers for minimizing damage in case of fire.

Separation involves dispersing key assets so that catastrophic events at one location affect the business only at that location. If all assets were in the same place, the business would face more serious issues. For example, a company utilizes a geographically diverse workforce so that production may continue when issues arise at one warehouse.Duplication involves creating a backup plan, often by using technology. For example, because information system server failure would stop a company's operations, a backup server is readily available in case the primary server fails.

Diversification allocates business resources for creating multiple lines of business offering a variety of products or services in different industries. A significant revenue loss from one line will not result in irreparable harm to the company's bottom line. For example, in addition to serving food, a restaurant has grocery stores

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 4 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

carry its line of salad dressings, marinades, and sauces.

Risk management framework

All companies face risks. Without taking some degree of risk, they may have little chance of staying competitive. On the flip side, taking too much risk can lead to business failure. An effective risk management framework aims to strike the proper balance, protecting the organization's capital and earnings without hindering its growth. In addition, investors are more willing to invest in companies with good risk management practices. This generally results in lower borrowing costs, easier access to capital, and improved long-term performance.

Risk Identification

The first step in analysing the risks a company faces is to define the risk universe. The risk universe is simply a list of all possible risks. They may fall into such categories as operational risk, regulatory risk, legal risk, political risk, strategic risk, information technology (IT) risk, and credit risk. After listing all its possible risks, the company can then select the risks to which it is most exposed and divide them into core and non-core risks. Core risks are those that the company must take in order to drive performance and long-term growth. Non-core risks are often not essential and can be minimized or eliminated completely.

Risk Measurement

Risk measurement provides information on the amount of either a specific risk exposure or an aggregate risk exposure and the probability of a loss occurring due to those exposures. When measuring a specific risk exposure, it's important to consider the effect of that risk on the overall risk profile of the organization. For example, some risks may provide diversification benefits, while others may not. Another important consideration is the ability to measure exposure. Some risks are easier to measure than others. For example, market risk can be measured using observed market prices, but measuring operational risk is considered both an art and a science.

Risk Mitigation

Having categorized and measured its risks, a company can then decide on which risks to try to eliminate or minimize, and how many of its core risks to retain. Risk mitigation can be achieved through such means as an outright sale of assets or liabilities, buying insurance, hedging with derivatives, or diversification. Companies have more direct control over certain kinds of risks than others, but they need to attempt to mitigate against all of the significant ones.

Risk Reporting and Monitoring

It is important to report regularly on specific and aggregate risk measures in order to ensure that risk remains at an acceptable level. Financial institutions that trade daily will produce daily risk reports. Other kinds of enterprises may require less frequent reporting. Risk reports must be sent to risk personnel who have the authority to adjust (or instruct others to adjust) risk exposures.

Risk Governance

Risk governance is the process that ensures all company employees perform their duties in accordance with the risk management framework. Risk governance involves defining the roles of all employees, segregating duties, and assigning authority to individuals, committees, and the board for approval of core risks, risk limits, exceptions to limits, and oversight in general.

Compliance risk

Running a business is inherently risky. Any business practice that doesn't follow the law or industry rules is a compliance risk. When an organisation isn't compliant, it risks potential financial, legal and other losses. For example, if an organisation fails to comply with data regulations, it can be fined or face lawsuits when a cyber attacker steals data.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 4 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

When building infrastructure, protecting data should be a top priority. This means writing coding rules, developing databases and setting up application procedures, all with data safety in mind. Organisations typically set their security controls to meet regulatory standards for HIPAA, PCI-DSS, SOX, GDPR and others.

Best practices for data integrity provide a roadmap for data safety. They include rules like who can access data. Smaller organisations that are unfamiliar with best practices should seek guidance from an expert.

Common Types of Compliance Risk

The best way to limit risk is to find your weak links. Human error, server misconfigurations or even an oversight in application logic are compliance risks. Here are some common compliance risks:

Human error: Phishing and social engineering succeed because people make mistakes. If employees are not regularly trained on common cyber threats, your data is at risk.

Lack of monitoring: Compliance regulations often require data monitoring. With monitoring, administrators can identify active threats and get alerts when there's a data breach. Both of which can lessen the severity of a breach and subsequent fines.

Improper storage: Sensitive data should be stored in encrypted form. Using cleartext format puts your organisation at greater risk if there's a data breach.

Failure to audit access: Only authorised and authenticated users should have access to data. Every time someone accesses data it should be logged. These audit trails are not only useful in forensic analysis of data breaches, but they're also required by regulations like HIPAA.

Misconfigurations: Simple misconfigurations can lead to severe data breaches. Before deployment to production, test configurations across the whole environment.

Examples of Compliance Risk

Security missteps often cause or contribute to compliance risk. Often, administrators can't see how users are working with data. They also don't have visibility into how tools are protecting data. Here are two common compliance risks:

Not keeping software patched and updated. Cyber attackers often exploit vulnerabilities in outdated software. When a server's operating system remains unpatched after an update is released, the organisation becomes non-compliant. A good example of this risk is the Equifax data breach. There, outdated software allowed attackers to steal millions of user records.

Not auditing data access. If a person calls into customer service to discuss their credit card account, each representative who interacts with that data should be tracked. An audit trail ensures access to data can be checked and assessed. A trail is also important during and after a data breach for forensic analysis.

Strategic risk

Strategic risk is the possibility that a company's business decisions could lead to failure. These risks can be internal or external, and they can have a significant impact on an organization's ability to achieve its goals. Strategic risks can be a major factor in determining a company's value, especially if the company experiences a sudden decline in a short period of time.

Some examples of strategic risk include:

Reputational risk

The risk that a company's standing is threatened, such as through regulatory compliance breaches, shareholder activism, or poor public ratings

Governance risk

The risk that poor governance, risk, and compliance processes within an organization could have an impact

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 4 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Financial risk

The risk that relates to an organization's financial health, such as the risk of selling a large portion of the business to improve operational costs

Economic risk

The risk that the broader economic landscape could affect the success of a business strategy

Some ways to identify strategic risk include: Brainstorming in a group, Conducting a team-based exercise, Interviewing key stakeholders, Sending out a survey, and Using different types of analyses.

Conclusion

The focal point of the study is risk management in life insurance with emphasis on life insurance fraud. Increase in number of life insurance fraud hinders the business and therefore there is a need to focus on risk management. Risk management will not only help in discovering life insurance frauds but it will also help in controlling. Broadly the objectives of the study are to find out the types of life insurance fraud, understand the fraud control mechanism, measures to prevent life insurance fraud and to understand the customer's perception with regard to life insurance fraud. The following chapters deal in details about the study.