CONSTRUCTING OPERATIONAL RISK MATRICES FROM ORGANIZATIONAL BUSINESS PROCESSES USING A FUZZY AHP METHOD

CAMILA SOLÍS TORO.

Management Engineering

P.h.D. Juan Alejandro Peña Palacio

UNIVERSIDAD EIA
Finance
Envigado
2019

AKNOWLEDGEMENTS

I thank my bachelor thesis director Alejandro Peña and the researchers Alejandro Patiño and Christian Lochmueller for helping me throughout the process by answering all my questions and concerns, and for their time and commitment.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ANNEXES

RESUMEN

La globalización y el avance de la tecnología ha hecho que las organizaciones financieras principalmente y en general todas las entidades estén interconectadas entre sí a través de sistemas tecnológicos que facilitan la comunicación con los clientes, los proveedores, el mercado; con todos los grupos de interés.

De manera que a media que pasa el tiempo los sistemas evolucionan y se vuelven más complejos, haciendo a las organizaciones más vulnerables a los ciberriesgos y generando un sin fin número de retos de gestión. Gracias a la incertidumbre con la que se dan los ciberriesgos, las entidades financieras han optado por la contratación de seguros que les permitan cubrirse ante ellos; sin embargo, la estimación del valor en riesgo (VaR) que indica el valor que las pólizas deben cubrir por ciberriesgo sigue siendo todo un desafío, como se explica en el marco de referencia de este trabajo (McNeil, Frey, & Embrechts, 2015).

De modo que en este trabajo de grado se propone un modelo AHP neuronal borroso, para el cálculo del VaR derivado de actividades de ciberseguirdad en una entidad financiera, integrando en un solo modelo, no solo el criterio de expertos, sino una serie de matrices borrosas de gestión e impacto. Finalmente, dando como resultado el efecto que tienen diferentes niveles (ninguno, débil, medio y fuerte) de gestión sobre el VaR para el ciberriesgo en una entidad financiera.

ABSTRACT

Globalization and technological breakthroughs have brought the interconnection of institutions; technological systems enable communication with customers, suppliers and the market, with all the stakeholders. Therefore, as time passes, systems evolve and become more complex, making organizations more vulnerable to cyber risks and generating a never-ending number of management challenges.

Due to the uncertainty in which cyber risks occur, financial institutions have opted to buy insurance to cover them. However, the estimation of the value at risk (VaR), which designates indicates the value the insurance policies must cover concerning cyber-risk, still remains a challenge (McNeil et al., 2015).

Thus, in this bachelor thesis a fuzzy neuronal AHP model is proposed for the VaR calculation derived from cybersecurity activities in a financial entity. The proposed model integrates in a single model, not only the expert's criterion, but also fuzzy management and impact matrices. Finally, the influence of different levels of management on the VaR for cyber risk in a financial institution, will be presented.

INTRODUCTION

Risk impacts organizations worldwide. Therefore, in the course of history, some practices have emerged for risk prevention. These are gaining more relevance day by day, due to the characteristics of our uncertain and changing world. Each country has its own policies regarding risk, as different types of industries and enterprises exists in different countries. Each organization is in charge of adjusting the policies according to the local requirements and consequently, in its own way, without trespassing the laws stated by each authority. Although there are many techniques for operational risk management (ORM), a risk matrix is one of the most easily and highly used. These are often applied only with expert's knowledge, knowing that there are methods like fuzzy AHP that can enhance the reliability of this technique.

This bachelor thesis will focus on cyber risks, which are a type of operational risks(Accenture, 2016b). Cyber risk can be defined as a potential loss or harm related to technical infrastructure or the use of technology within an organization, which can result from human error, system and software flaws, criminal activity and other (RSA, 2016). Globalization and technological breakthroughs have brought the interconnection of institutions. Technological systems enable communication with customers, suppliers and the market and with stakeholders. Therefore, as time passes, systems evolve and become more complex, making organizations more vulnerable to cyber risks and generating a never-ending number of management challenges (Rohmeyer & Bayuk, 2019). Due to the uncertainty in which cyber risks occur, financial institutions have opted to adquire insurance to cover them. However, the estimation of the value at risk (VaR), which designates the value the insurance policies must cover owing to cyber-risk still remains a challenge (McNeil et al., 2015).

The model, which I propose in this work, allows the representation of the random variables of frequency and severity that define a risk event of operational risk. It handles cyberrisk as a linguistic random variable. The construction of the management and impact matrices happens through an Analytical Hierarchical Processe (AHP). The integration of experts judgment in cyber-risk, as well as the estimation of the OpVar for different management matrices, is done by using a fuzzy neural structure, obtained by the adjustment and learning of the aggregate loss distribution (LDA). The concept of LDA was established by the Basel Committee of Banking Supervision (BCBS) for the estimation of this risk (Basel Committee on Banking Supervision, 2009).

The first step in the analysis and validation of the proposed model was to construct a risk management matrix. The structure for the design of this matrix mixes methods for decision making with the principles of fuzzy logic. Initially, the qualitative variables that make up a cyber program management will be modeled according to the hierarchical decision tree that is defined for them. The preference of three experts will be integrated into the model when comparing each of the levels of the hierarchical decision tree and the resulting weights will refer to the severity, given that they represent the relative importance of each element in the decision. At the same time, five experts will answer a questionnaire referring to the frequency of the same qualitative variables that make up a cyber program management. Given the high quantity of qualitative information that these variables store, these will be modeled by using the principles of fuzzy logic.

The second step was to develop the impact matrix. For this, a database of a corporation that contains the daily transactions carried out at ATMs of the financial institution was used. The database includes the value of each transaction, the failed transactions and the respective cost generated. With these data, severity and frequency of risk events are determined. Based on this information the 5x5 impact matrix with 5 risk levels was constructed after using the k-means clustering process to obtain five k means for each distribution and using them to find the Euclidean distance between al 25 k-means combinations that indicate to which quadrant of the matrix does each set of data (severity, frequency) belong.

The third step was to use the computational intelligence toolbox to construct the fuzzy neural structure of the model, in accordance with the aggregated loss distribution (LDA), a concept defined by the Basel II accord set by The Basel Committee on Banking Supervision (BCBS). This toolbox uses the input linguistic variables of frequency and severity, and the management and impact matrices to obtain the LDA distribution as a result of a convolutional process between the fuzzy sets that describe the frequency and severity as random variables.

Finally, this work validates the proposed model taking into account the behavior of the aggregated loss distribution and capital requirements. The management matrices were constructed in terms of a series of activities aimed at the mitigation of cyber risk in a financial institution. Three matrices or management scenarios where defined: scenario E3 (Strong Management), scenario E2 (Moderate Management) and scenario E1 (Weak Management). At this stage, we expect that as the management becomes stronger the heavy tailed aggregated loss distributions (LDA) becomes slenderer, and the asymmetry or skewness coefficients tend towards increasingly higher positive values.

1 PRELIMINARY

1.1 PROBLEM FORMULATION

Nothing is set in stone; the world is constantly changing and businesses have to adapt to new circumstances to survive and thrive in the new environment that is evolving. Therefore, companies have to get ahead of facts, preventing losses that the future might carry. Organizations are exposed to risk with their operations. This kind of risk is called operational risk. “Risks affecting organizations can have consequences in terms of economic performance and professional reputation, as well as environmental safety and societal outcomes. Thus, managing risk effectively helps organizations perform well in an environment full of uncertainty” (ISO, 2009). As a rule, effective operational risk management “requires the evaluation of events in a two-dimensional approach. On the one hand, from the perspective of the uncertainty occurrence [probability], and on the other from the viewpoint of the effect or result [impact]”(IACOB, 2014).

Levine (2012) affirms that a “risk matrix is a common used tool throughout the public and private sector” to assess, manage and control semi-quantitative risk (Markowski & Mannan, 2008). Therefore, “one side of applying a risk matrix method is based on using qualitative risk parameters [subjective process], the other side is based on using numerical interpretation of risk parameters by means of crisp intervals [quantitative process]” (Abul-Haggag & Barakat, 2013). In other words, a risk matrix is an analysis technique that assesses risk, by assigning a probability that represents the likelihood of an event or consequence happening. Then, it is leveled into a category of probability. The same steps are carried out with regard to the outcome (impact). Thus, showing the estimated magnitude of a risk. With this procedure, analysts can have a better understanding of risk and its effects within their organizations. Hence, improving decision making in terms of easier and more accurate decisions.

Most problems do not have a single answer, there can be multiple procedures for an activity and this is where the AHP process is relevant to complete the task. “The analytic hierarchy process (AHP) is one of the most widely-used multi-attribute decision-making (MADM) methods” (Demirel, Demirel, & Kahraman, 2008). Wind & Saaty (1980) state that with a systematic and logical approach you can analyze complex decisions. Also, Badri (2001) “addresses how to determine the relative importance of a set of activities in a multi-criteria decision problem” within the AHP process. “The fuzzy set theory makes it possible to incorporate judgments on intangible qualitative criteria alongside tangible quantitative criteria [allowing] decision makers to incorporate unquantifiable information, incomplete information, non-obtainable information and partially ignorant facts into decision mode” (Kulak, Durmuşoğlu, & Kahraman, 2005). That is why this method is “capable of capturing a human’s appraisal of ambiguity” (Erensal, Öncan, & Demircan, 2006) and to deal with uncertainty.

Countries with financial institutions, like banks and assurance companies, have a governmental entity in charge of inspecting and monitoring operational risk within organizations. In Colombia, the agency is called the Superintendencia Financiera de Colombia (SFC).

The SFC states that entities must develop, establish, implement and maintain an Operational Risk Management System (SARO), according to their structure, size, corporate purpose and support activities. The latter carried out directly or through third parties, which allows to effectively identify, measure, control and monitor this risk. This system consists of minimum elements (policies, procedures, documentation, organizational structure, registration of operational risk events, control bodies, technological platform, information dissemination and training) through which effective risk management is sought. Before implementing this system, organizations must establish policies, objectives, procedures, and structure for operational risk management, these must be aligned with the strategic plan of each entity for it to work correctly (Superintendencia Financiera de Colombia, 2006).

According to the reviewed literature, the importance of risk and its impact in organizations and worldwide is essential. Therefore, in the course of history, some practices have emerged for risk prevention, taking more relevance every day, due to the characteristics of an uncertain and changing world. Each country has its own policies regarding risk. However, due to different types of industries and enterprises, each institution is in charge of adjusting the policies in its own way, without trespassing the laws stated by each authority. Although there are many techniques for operational risk management (ORM), a risk matrix is one of the most easily and highly used (Anthony TonyCox, 2008), it is often applied only with expert's knowledge, knowing that there are methods like fuzzy AHP that enhance the reliability of this technique (Zhou & Thai, 2016).

Thus, it is important to describe a method for building operational risk matrices according to the characteristics of an organization's business operations, following the parameters of operational risk and using fuzzy AHP method. As a result, my inquiry is how to build risk matrices based on the characteristics of business operations of an organization using a fuzzy AHP method?

1.2 PROJECT OBJECTIVES

1.2.1 General Objective

Developing a model to construct operational risk matrices according to the characteristics of an organization's business operations using a fuzzy AHP method.

1.2.2 Specific Objectives

1. Analyze parameters and variables that make up the AHP.
2. Design a model for the use of operational risk management matrices using the structure of a fuzzy AHP model.
3. Develop the proposed model through the use of dot net technologies and interoperable Microsoft Excel functions.
4. Validate the model taking into account the behavior of the aggregated distribution of losses and capital requirements.

1.3 THEORETICAL FRAMEWORK

1.3.1 Background

Effective risk management requires the identification, management, measurement, monitoring and control of both opportunities and risks, so that instead of managing the downside of risks they can focus on new opportunities and continue to success while creating value (Bekefi, Epstein, & Yuthas, 2011).

According to Abul-Haggag & Barakat (2013) before determining the appropriate measures to control risk it's important to know which level of risk is acceptable and which controls would cost-effectively reduce risk. As a result, the preliminary stage for hazard prevention is risk assessment (Hsu, Huang, & Tseng 2016), which can be accomplished by means of qualitative and quantitative methods. A risk matrix "is a subjective risk assessment tool, that combines the severity of the consequences occurring in a certain accident scenario and its frequency" (Abul-Haggag & Barakat, 2013).

> Also, the risk of operational safety can be assessed based on a fuzzy AHP approach, comparing the traditional risk matrix with a discrete scale, and the revised risk matrix with a continuous scale for assessing risk factors. The revised risk matrix may provide theoretical references for methodological researchers in risk assessments. In conclusion, the fuzzy AHP approach can raise the measurement validity of subjects, leading to improve the performance of a risk matrix (Hsu, Huang, & Tseng 2016).

Basically, fuzzy logic deals with uncertainty in risk assessment, making a fuzzy risk matrix more precise and reliable than a traditional risk matrix (TRM) (Markowski & Mannan, 2008).

Risk evaluation is vital in all industries, but it plays a critical role in some sectors. For example, a leakage from a natural gas pipeline may lead to a catastrophic disaster and substantial economic losses because natural gas diffuses and combusts easily. Therefore, an effective method for a comprehensive risk evaluation can help pipeline management define risk levels, identify risk factors, assess their consequences and reduce risk. First, using AHP, risk factors are categorized in a hierarchy according to their impact level. Then, the fuzzy method converts natural linguistic expressions into failure or risk probabilities; and finally, a risk matrix is constructed with the probability and consequence or severity of the accident (Lu et al., 2015).

Another example is the use of a risk matrix for safety assessment in hospitals. This methodology involves searching and identifying potential risks, which would later be classified into levels; providing an opportunity for self-evaluation, preventing accidental exposures and managing the safety measures that are most suitable for each hospital's conditions (Vilaragut et al., 2013).
Wang, Chan, Yee, & Diaz-Rainey (2012) implement a risk assessment model by using fuzzy AHP to calculate aggregated risk in various green initiatives in the supply chain of the fashion industry. As a result, they obtain a structured analysis of aggregate risk, which will improve the decision-making process. Nevertheless, this method can be applied to other industries while preserving the hierarchical structure but modifying it according to the nature of the organization.

> Last but not least, the AHP method serves as a tool for checking and reducing the inconsistencies of safety risk severities assigned by the expert. The framework decomposed the decision problem into a hierarchy of more

> easily comprehended sub-problems that enhance the assignment of weights to the criteria and sub-criterions. (…) AHP (...) provides a robust method for prioritization of safety risks (...). This method assists in a safety risk assessment and accident/injury prevention process; a framework that reduces biased decision making while facilitating consensus decision making by a group of decision makers (Aminbakhsh, Gunduz, & Sonmez, 2013).

According to the above, it is shown that a risk matrix that uses a fuzzy AHP is a highly reliable tool that can be applied to multiple industries. However, after the revision of the literature it becomes clear that finding guidelines for such a method is a very challenging task. This is due to the fact that most papers and articles apply one of all the methods described above, according to the type of institution or industry and the occurrence of a particular event. Therefore, a methodology will be proposed for the construction of operational risk matrixes based on the principles of fuzzy logic and decision-making methods like AHP.

1.3.2 Operational Risk

> The Bank for International Settlements (1998) defined operational risk, "as the risk of loss arising from various types of human or technical error; which involves breakdowns in internal controls (failure of information technology systems) and corporate governance. Such breakdowns can lead to financial losses through error, fraud, or failure to perform in a timely manner or cause the interests of the institution to be compromised in some other way".

Thus, an important type of risk in risk management is operational risk, and its increasing importance within the context of modern financial markets, globalization and changes in industries overall.

The Basel Committee in collaboration with the industry has identified seven types of operational risks that may result in potential losses (Basel, 2003).

First, internal fraud, which includes acts that are committed internally in an organization, which can be in form of defraud, misappropriation of assets, forgery, embezzlement, bribes, deliberate mismarking of positions, theft and circumvent the law, the company policies or regulations. For example: employee theft, insider trading without the firm's knowledge, account takeover, impersonation, tax noncompliance, malicious destruction of assets, etc. (Basel, 2003).

Second, external fraud, which is the same as internal fraud, with the difference that the loss is due to acts committed by third parties. For example, hacking or acquiring unauthorized information, theft, robbery, forgery etc. (Basel, 2003).

Third, employment practices and workplace safety, which includes losses that can arise from noncompliance with employment, health, safety laws or agreements, payment of personal injury claims, diversity or discrimination. For example, unethical termination criteria, violation of employee health and safety rules, organized labor activities, etc. general liability (Basel, 2003).

Fourth, clients, products and business practices, refer to losses caused by events where the organization fails to honor professional commitments, like promises made to their clients. For example, fiduciary breaches, misuse of confidential customer information, suitability issues, market manipulation, money laundering, sale of unauthorized products and unlicensed activities (Basel, 2003).

Fifth, damage to physical assets, consider losses incurred by damages caused to physical assets owing to natural disasters or other events like terrorism and vandalism. In some cases, vandalism or acts involving the deliberate destruction or damage to public or private property can include fires, flood and others, that can also be caused by nature (Basel, 2003).

Sixth, business disruption and system failures. These include hardware and software failures, telecommunication problems, and utility outages. These events are more common nowadays due to the advances of technology and the integration between systems (Basel, 2003).

Seventh, execution, delivery and process management failures, which refer to losses originated by failure in delivery, transaction or process management. For example, data entry errors, collateral management failures (miscommunication, deadline misses, accounting errors, inaccurate reports, incorrect client records, etc.), incomplete legal documentation, unapproved access given to client accounts, , negligent loss of client assets and vendor disputes (Basel, 2003).

In Colombia the SFC established that financial entities can develop their own operational risk measurement models, for which it establishes a period of three to five years of loss data for this type of risk. Since operational loss events are infrequent, the Basel Committee recommends using scenarios as a method for measuring risk if historical data is insufficient.

The Basel Committee provides three approaches for the measurement of the capital charge for operational risk: The Basic Indicator Approach (BIA), the Standardized Approach (SA), and the Advanced Measurement Approaches (AMA). Because the BIA and the TSA fail to estimate correctly the operational risk capital requirements of a wide spectrum of banks the Committee recommends the use of the AMA approach, because it requires a greater amount of information from an organization's business operations. Furthermore, the estimated regulatory capital is usually lower when applying AMA in comparison to the other two approaches.

Within the AMA models, three methodologies stand out: Internal Measurement Approach – IMA, Loss Distribution Approach – LDA and Score Card Approach (Valová, 2011).

The goal of operational risk quantification is to determine the aggregate distribution of operational losses that occur during a specific period of time. When the aggregate loss distribution is obtained, risk-adjusted performance measures can be calculated and decisions about capital allocation and risk hedging can be taken. Operational risk measurement systems must be based on four elements: internal data, relevant external data, scenario analysis, and factors reflecting the business environment, and the internal control systems (Cruz, Peters, & Shevchenko, 2015).

According to Basel Committee on Banking Supervision (2006), the most common risk measure in risk management is the Value at Risk (VaR). The Operational Value at Risk (OpV) is a statistical measure expressed in terms of monetary units derived from the loss distribution. This indicator helps to measure an entity's risk exposure. It represents the maximum potential loss that an institution could incur due to operational risk during a fixed period of time (normally one year), and with a confidence level of 99.9% according to Basel II (Jiménez Rodríguez, Feria Domínguez, & Martín Marin, n.d.).

Under the Accord (Basel II), the Committee requires banks to demonstrate their ability in capturing potentially severe tail loss events. To be more precise, banks should put an operational risk capital aside in line with the 99.9% confidence level over a one-year holding period (Embrechts, Hansj¨, Furrer, & Kaufmann, n.d.).

The OpRisk capital charge represents the regulatory minimum capital required as a contingency or provision for operational risk. Risk managers need to calculate the regulatory capital requirement VaR0.999 as the sum of expected losses (EL) and unexpected losses (UL). Expected losses are the usual or average losses that an organization incurs in normal operational conditions. Whereas, unexpected or unanticipated losses are deviations from the average that may unbalance the stability of an organization. That means, expected loss is the mean of the loss distribution (E(S)), and unexpected loss is the difference between the OpV and the expected loss, as shown in *Figure 1* (Cruz, Peters, & Shevchenko, 2015).

The first step to establish an appropriate level of capital to cover unexpected losses of operational risk is to determine the confidence level. A confidence level is a statistical concept expressed as a percentage. This percentage corresponds to the degree of certainty that the likelihood or consequence score assigned reflects the reality of the business and the assessed risk. The higher the confidence level the more accurate the calculation of the (VaR) will be. However, in practice it is not possible to establish a confidence level of 100%, because risk managers are not completely sure that VaR will fall within the confidence interval, given that the loss distributions are not a perfect cause. They are usually calculated based on incomplete or altered historical data (Navarrete, 2006). Nevertheless, risk managers use confidence levels within a range from 95 % to 99 % and higher, taking into account that "Basel II requires a 99,9 % percentile confidence interval, this means taking the 10th largest loss in 10,000 losses obtained by running a simulation" (Basel Committee on Banking Supervision, 2006).

Once the confidence level is defined to cover unexpected losses, the calculation of the corresponding amount of capital involves the following steps:

i. Identifying frequency and severity distributions from the data;
ii. Combining both distributions to obtain an aggregate loss distribution;
iii. "Obtaining operational Value at Risk (OpV) by taking the percentile of the aggregate loss distribution at the desired confidence level (Navarrete, 2006).

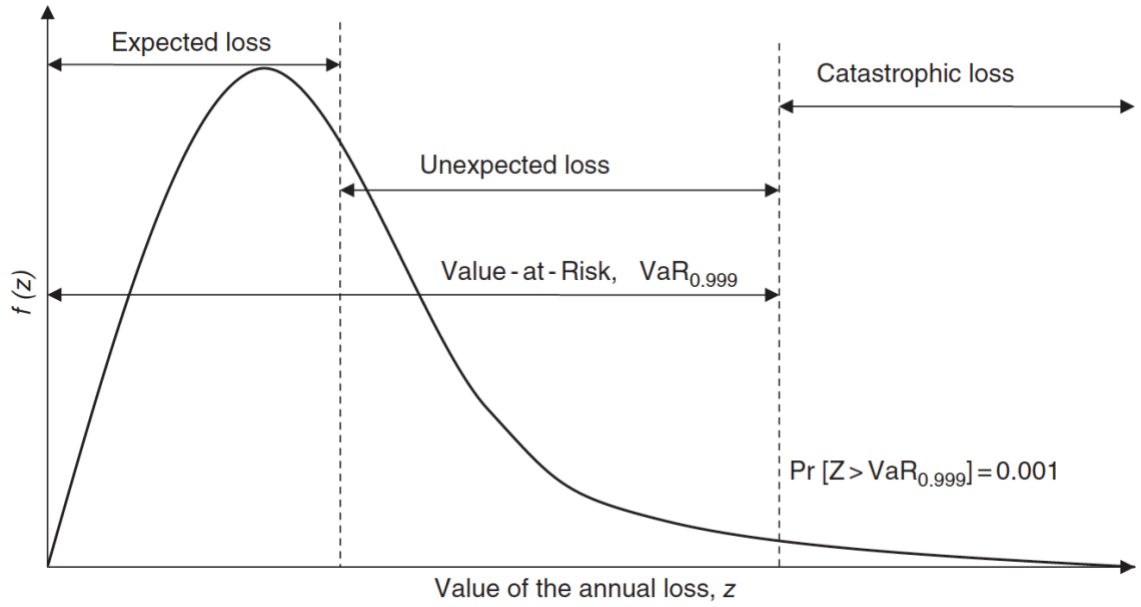


Figure 1: The loss distribution shows expected loss, unexpected loss and VAR

Retrieved from: (Cruz et al., 2015)

Considering S as the aggregated loss distribution, it can be deduced that when:

- $S \geq 1$, there has to be substantial management
- $S = 1$, there has to be standard management
- $S < 1$, there is no need of management

In operational risk, the calculation of unexpected loss is more complex since it involves the frequency and severity components of the loss distribution. Frequency refers to how often a loss event occurs. It is measured in terms of a number of events per time units and it is described by a discrete distribution. Whereas severity depends on the monetary impact of the event and is described by a continuous distribution (Cruz et al., 2015).

To combine severity and frequency distributions, two approaches exist: Closed form and open from. Closed form solutions involve solving analytical formulas such as integrals and equations. One closed form solution is convolution, which is used when we need to calculate the distribution of the sum of independent random variables such as the aggregate loss, it combines the frequency and severity distributions to produce a third function (Cruz et al., 2015; Navarrete, 2006).

> An alternative method to combine both distributions (still closed-form) is not to deal with them directly, but to take some transformation that allows manipulating the distributions more efficiently. Such a transformation is the Fourier transformation, which operates in the frequency domain. This approach involves dealing with trigonometric functions (such as sines and cosines), and complex numbers. Since Fourier transforms are multiplicative, once we obtain the transforms of the distributions, we obtain their product (an easier operation than convolution). To obtain the aggregate loss distribution we take the inverse Fourier transform of this product (Navarrete, 2006).

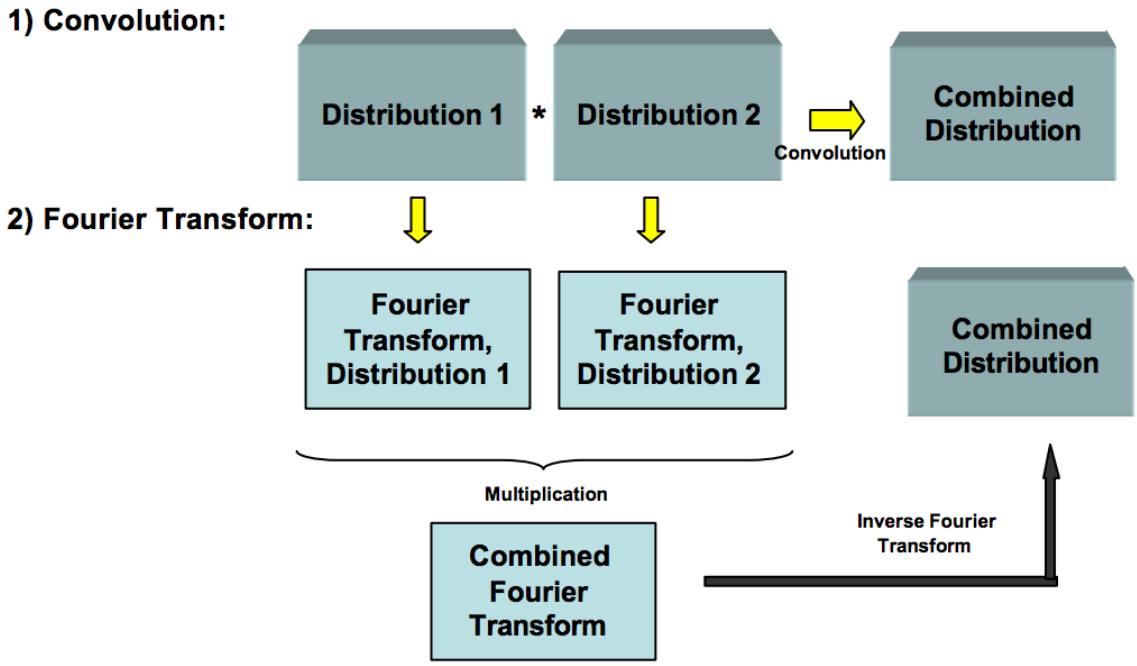


Figure 2: Comparison of Convolution and Fourier Transforms
Retrieved from: (Navarrete, 2006).

On the other hand, in open form solutions, an algorithm is implemented in a computer to obtain the loss distribution at once. Monte Carlo simulation is the most renown and used of these methods because it is the easiest to implement, it simulates different scenarios for frequency and severity by generating random numbers using both, the frequency and the severity distributions identified from in the historical data of a company (Cruz et al., 2015; Navarrete, 2006).

However, Monte Carlo Simulation is typically slow, thus Fourier is also widely used. Even though it has a long history, its applications to computing very high quantiles of the compound distribution functions with high frequencies and heavy tails are only recent developments and various pitfalls exist (Cruz et al., 2015).

1.3.3 Risk Matrix

A risk matrix is a widely used risk management tool (Jan Duijm Duijm & Jan, 2015) that combines qualitative or semi-quantitative ratings of consequence and probability to produce a level of risk (ACME Business Consulting. Inc., 2017). Risk matrices represent risks graphically, helping risk managers rate and prioritize risks for decision making, taking into account the organizations risk tolerance (ACME Business Consulting. Inc., 2017).

To build a risk matrix with the accurate parameters, it is necessary, first to identify the risk. Risk can be defined, as the likelihood of an event happening that will have an effect on the organizational objectives, making their achievement uncertain. Therefore, it is of vital importance to describe risk accurately and comprehensively, studying which areas or area of the organization is affected, in order to create an effective approach to risk management (Health Service Executive, 2011).

The second step according to Health Service Executive (2011) is risk analysis, which refers to the development and understanding of the risk acknowledged. When analyzing risk, it has to be measured in terms of likelihood (frequency) and impact (severity or consequence). Both elements are determined when assessing the level of risk. Frequency refers to how often a risk occurs. It is measured in terms of a number of events per time units and is described by a discrete distribution. Severity usually depends on the monetary impact of an event, but it can also be the outcome of a given event and is described by a continuous distribution.

The methodology for measuring risk plots a value of likelihood against a value of impact (consequence), reducing risk to a single and easily comparable value. The risk score is calculated by multiplying the consequence by the likelihood: C (consequence) × L (likelihood) = R (risk score) (National Patient Agent Safety, 2008).

It is necessary to define the category and scale of the severity and frequency of an event (Markowski & Mannan, 2008).

The categories below represent the likelihood of the occurrence of a risk. The likelihood scores on a scale from 1 – 5:

1. Rare: exceptional risks, which have a chance of occurrence less than 10%.

Examples:

- Pandemic impacts portion of global workforce.
- Widespread damage to electrical grid from solar flares.

2. Unlikely: risks that have a low probability of occurrence but still cannot be ruled out completely.

Examples:

- Hot site experiences outage at the same time as the primary site.
- Multiple, important system administrators quit at the same time.

3. Possible: risks, which have a near 50/50 probability of occurrence.

   Examples:

   - Unauthorized change to a production application prevents the company's ability to process credit cards.
   - 5+ year old server will experience a catastrophic hard drive failure.

4. Likely: risks that have 60-80% chances of occurrence can be grouped as likely.

Examples:

- Users will open phishing emails and infect their workstations with malware.
- Team working on a project will overwrite data and require files to be restored from backup.

5. Almost Certain: risks that definitely would show-up with a chance of occurrence of more than 80%.

   Examples:

- User will have a laptop or smart phone lost or stolen.
- The company's external web presence will be probed/attacked by hackers

The consequences of a risk can be ranked and classified into one of the five categories, based on how severe the damage can be.

1. Insignificant: there is little-to-no impact to business operations.
   Examples:
   - Financial impact is less than $[MINOR RISK VALUE].
   - Performance or availability of up to Business Essential systems, assets and data is minimally impacted.
   - Isolated staff dissatisfaction.
     (ACME Business Consulting. Inc., 2017)

2. Minor: there are marginal impacts to business operations, the extent of damage is not too significant and is not likely to make much of a difference.
   Examples:
   - Financial impact is less than $[MODERATE RISK VALUE].
   - Performance or availability of up to Business Essential systems, assets and data is moderately impacted.
   - Local, short-term, negative media coverage.
   - Department-level staff morale problems.
     ACME Business Consulting. Inc., 2017)

3. Moderate: there are serious impacts to business operations, which do not impose a great threat, but yet the sizable damage can be classified as moderate.
   Examples:
   - Financial impact is less than $[MAJOR RISK VALUE].
   - Performance or availability of Mission Critical systems, assets and data is minimally impacted.
   - Performance or availability of up to Business Essential systems is significantly impacted.
   - A contractual, statutory and/or regulatory requirement is violated.
   - National, short-term, negative media coverage.
   - Widespread staff morale problems and increase in turnover.
     (ACME Business Consulting. Inc., 2017)

4. Critical: there are critical impacts to business operations, risks with significantly large consequences, which can lead to a great amount of loss.
   Examples:
   - Financial impact could exceed $[CRITICAL RISK VALUE].
   - The organizations reputation and/or competitive position will be damaged.
   - Performance or availability of Mission Critical systems, assets and data is significantly impacted.
   - Performance or availability of up to Business Essential systems, assets and data is impacted to the point of being unusable.

- A contractual, statutory and/or regulatory requirement will be violated, where some level of punitive action would be an expected outcome.
- International, long-term, negative media coverage with noticeable loss of market share.
  (ACME Business Consulting. Inc., 2017)

5. Catastrophic: there are catastrophic impacts to business operations, which can make the organization unproductive and must be a top priority during risk management.
   Examples:
   - Financial impact could exceed $[CATASTROPHIC RISK VALUE].
   - The organizations reputation and/or competitive position will be severely damaged.
   - Performance or availability of up to Mission Critical systems, assets and data is impacted to the point of being unusable.
   - Key technologies will not be available and there are no alternatives.
   - A contractual, statutory and/or regulatory requirement will be violated, where significant punitive action would be an expected outcome.
     (ACME Business Consulting. Inc., 2017)

Risk categorization takes place once the risks have been placed in the cells the risk matrix, corresponding to the appropriate likelihood and consequences. This helps management compare and prioritize risks. According to Anand & Sameera (2012) each of the risks placed in the table will fall under one of the following four levels of risk: low, moderate, high, extreme.

1. Low Risk:

Represents the risks that fall in the green cells and can be ignored as they usually do not pose any significant problem or can be manage with routine procedures.
Examples:

- Financial impact is negligible (less than $[MODERATE RISK VALUE]).
- Impact would not be damaging to the organizations reputation or impede business operations.
- There are no violations of contractual, statutory or regulatory requirements.
  (ACME Business Consulting. Inc., 2017)

2. Moderate Risk

Moderate risks are symbolized by the yellow cells, and even if they just represent minimal damage, it is best to implement monitoring or response procedures and develop risk management strategies in time. Such risks do not require extensive resources; rather they can be handled with smart thinking and logical planning.
Examples:

- Financial impact is potentially between $[MODERATE RISK VALUE] and $[MAJOR RISK VALUE].
- Impact would not be damaging to the organizations reputation or impede business operations.
- Impact could impede Business Core or Business Supporting systems or business operations.

- This may involve a violation of contractual requirements.
- There are no violations of statutory or regulatory requirements.
  (ACME Business Consulting. Inc., 2017)

3. Medium Risk:

The orange color represents this risk level. Moderate damage could occur. Thus, it requires action or risk management strategies.
Examples:

1) Impact could include damage to the organization's reputation.
2) Impact could impede Business Essential systems or business operations.
3) This may involve a violation of contractual, statutory and/or regulatory requirements.
4) Financial impact is potentially between $[MAJOR RISK VALUE] and $[CRITICAL RISK VALUE].
5) The organizations stock price could be negatively affected (<5% negative deviation).
   (ACME Business Consulting. Inc., 2017)

4. High Risk

Represents the risks that fall in the cells with the red color. They are the most critical risks and must be addressed with priority. They require immediate action as their effects could be devastating to the enterprise. Extensive financial and long-term brand damage could occur from a critical risk, for example:

- Impact could include extensive damage to the organization's reputation.
- Impact could impede Mission Critical systems or business operations.
- Impact could negatively affect the organizations long-term competitive position.
- Risk scenarios involving potential physical harm or fatality are included in this category.
- Financial impact is potentially over $[CATASTROPHIC RISK VALUE].
- The organizations stock price could be significantly affected (>10% negative deviation).
  (ACME Business Consulting. Inc., 2017)

Risk is visualized through the mapping of the two attributes of an adverse event (consequence, likelihood) to some value of risk. In the context of the risk matrix, the value of risk is a discrete value, corresponding to the categories of consequence and likelihood: "IF frequency is "f"' AND severity of consequences is "c" (as a category) THEN risk is "r" (category).

For example: IF frequency is "unlikely" and severity of consequence is "insignificant" THEN the risk category may be assessed as "low".

The procedure is more difficult for intermediate categories of severity and frequency. In such cases, an expert opinion is applied, using an interpolation scheme. Of course, such an opinion may be quite subjective and imprecise (Markowski & Mannan, 2008). Qualitative verbal descriptors, for example: low, high, or possible, are quite vague and imprecise. However, risk analysts frequently use them. They introduce uncertainty as a result of fuzziness, not randomness (Markowski & Mannan, 2008).

The risk matrix in *Figure 3* shows both numerical scoring and color bandings. Risk management identifies the level at which the risk will be managed, assigns priorities for remedial action, and determines whether risks are to be accepted, on the basis of the color bandings and/or risk score (National Patient Agent Safety, 2008).

	Likelihood				
Consequence	1	2	3	4	5
	Rare	Unlikely	Possible	Likely	Almost certain
5 Catastrophic	5	10	15	20	25
4 Major	4	8	12	16	20
3 Moderate	3	6	9	12	15
2 Minor	2	4	6	8	10
1 Negligible	1	2	3	4	5

For grading risk, the scores obtained from the risk matrix are assigned grades
as follows:

1–3	Low risk
4–6	Moderate risk
8–12	High risk
15–25	Extreme risk

Figure 3: Risk Matrix with likelihood and consequence
Retrieved from: (National Patient Agent Safety, 2008)

A risk matrix is a basis for further risk control measures, such as processes, policies, procedures, protocols, emergency arrangements, guidelines and engineering controls, preventative maintenance controls, protocols, training, team working, etc. All these measures are put in place to reduce or eliminate the risk.

1.3.4 Multi-Criteria Decision Making Methods

Multi-criteria decision making (MCDM) is an area that has allowed solving many real-life problems, for which there is no single element that determines an action to follow. For decision making there are three possible scenarios: low certainty, low risk and low uncertainty. The decisions under certainty are those that are made having full knowledge of what will happen, when selecting a solution alternative. The decisions under risk are those that have statistical data of the probability of occurrence of an event when selecting a solution alternative, and decisions under uncertainty are those that are made, when there is no information that helps in the selection of the best alternative (Baird, 1989).

Human beings face daily situations in which they need to make decisions correctly. Most of these decisions are made under uncertainty, without taking into account all the possible criteria and considering only a part of all the information available, this due to the inability of the human brain to process a large amount of complex information at the same time (Kubler et al., 2016). Some decisions may be simple to make when the consequences of making a bad decision are small. However, decisions with significant consequences need to be taken more seriously and methods must be used to guarantee a reasonable solution (Govindan & Jepsen, 2016).

The multi-criteria decision making (MCDM) methods allow to work with information of different criteria at the same time and to include information on expert judgments. These methods include ELECTRE (Elimination and Choice Expressing Reality), TOPSIS (Technique for Order of Preference by Similarity to Ideal Solution), VIKOR (Multicriteria Optimization and Compromise Solution), AHP (Analytical Hierarchy Process) and PROMETHEE (preference-ranking organization method for enrichment) (Danesh, Ryan, & Abbasi, 2017).

1.3.5 Fuzzy Logic Models

In recent years, the number and variety of applications of fuzzy logic have increased significantly. Fuzzy logic refers to things that are not clear or are vague, so it has the ability to solve problems related to the uncertainty or inaccuracies of any situation. It resembles human reasoning because it imitates the process of decision making in humans, which involves all intermediate possibilities between yes and no, thus is very understandable. Therefore, it ensures a wide field of applicability and high interest for industrial applications, present and future. The highlight of the fuzzy models is their ability to analyze the same problem in different ways, thus reaching several solutions that reflect multiple perspectives (Aliev, 2013).

A fuzzy model has two fundamental elements: linguistic variables and the rules of inference. The linguistic variables are the input and output variables, and they are described by a range of values and a set of qualities, usually specifically adjectives like “small,” “little,” “medium,” “high,” and so on are used. On the other hand, the rules of inference establish the relationship between the linguistic variables of input and output, through a series of inference rules that integrate the experience of an expert in a specific area of knowledge from which the linguistic variables come (Aliev, 2013).

The fuzzy logic system architecture is composed of three processes that allow the modeling of the information and, in general, the estimation of the LDA as described above. The first process is described as fuzzification, in this stage crisp numbers, which are the system inputs, are transformed into fuzzy sets by assigning a value to an input variable in terms of the qualities that describe it. Then, a set of inference rules, IF-THEN rules provided by the expert, allow to relate both the input and output variables in terms of their qualities. Finally, the defuzzification process converts the fuzzy sets obtained by using the inference rules into a crisp value. In other words, it allows the estimation of an output value in terms of the weighting of the inference rules according to the qualities that define the output linguistic variable (Aliev, 2013).

1.3.6 Cyber-Risk

Taking into account that the case study of this bachelor’s thesis is going to be in cyberrisk we broaden this topic further, from a conceptual perspective, in this section.

Organizations and more so banks are increasingly aware of the threats that can arise from cybercrimes (Deloitte, 2017), thus they are continuously strengthening their cyber-security, recognizing the reputational and monetary implications of cyber-attacks.

The financial sector is more exposed to cyber-risk than other sectors, because it is highly dependent on information as a key input and is IT-intensive. Also, given that financial institutions are interconnected with organizations from different sectors through the payment systems, it is critical that they possess an effective cyber security system to prevent the hole system being undermined by a cyber-attack (Crisanto & Prenio, 2017).

Within the financial sector, banks have the most public-facing products and services and their systems are in constant contact with outside parties, making them significantly vulnerable to cyber-attacks (Crisanto & Prenio, 2017). Also, according to Verizon's Data Breach Investigation Report of 2018, 76% of the breaches were financially motivated, so perpetrators are driven by financial gain, not espionage, fun, grudge or other (Verizon, 2018). This report reaffirms why banks are highly targeted and why it is important that they have adequate governance, systems, procedures and processes in place.

At present the question is when, not if, an institution will experience a cyber-attack. According to Accenture high performance report, even though across the banking industry 78% of senior security executives expressed confidence about their overall cybersecurity strategy, they face each year an average of approximately 85 serious cyber breaches, of which one third are successful (Accenture, 2016a). Deloitte's Global Risk Management Survey (Deloitte, 2017) showed that only 42% of respondents considered their organization to be extremely or very effective in managing cyber-risk. Nevertheless, often cyber-risk is ranked topmost among operational risk , according to Deloitte's Global Risk Management Survey (2017) 41% of the respondents said it was one of the top three risks that would increase the most in importance for their institution over the next two years, including 18% saying it was the number one risk . Hence, the approach companies use to protect themselves against cyberattacks is changing, because each day there are more potential entry points for attacks, they can't just build a strong perimeter, they have to detect what's more vulnerable and have adequate response plans in place.

The CPMI-IOSCO Guidance defines "cyber-risk" as "the combination of the probability of an event occurring within the realm of an organization's information assets, computer and communication resources and the consequences of that event for an organization" (Crisanto & Prenio, 2017). In other words, any natural or legal person with information assets that uses online communications technology is exposed to cyber-risk. The arrival of information technology (IT) has made interconnections of people and organizations within and across economies omnipresent, intensifying risk of cyber-attacks.

The CPMI cyber-security framework contains five processes identification, protection, detection, response and recovery. First, companies have to identify the threat profile, the risk exposure and the expected loss. Second, organizations protect by increasing internal and third party security. Third, entities detect these risks by making penetration tests and assessing it´s digital infrastructure and defense, by making a security assessment of applications and by doing periodical vulnerability scans. Fourth, companies respond taking into account pre-determined threat scenarios, for which they have run dynamic simulations assessing incident response readiness and effectiveness. Ultimately, business recovery, initiating stakeholder's continuity plans,

which involve action plans and mobilization of resources. “Hence, these include general requirements on governance and oversight, risk ownership and accountability, information security measures (patch management procedures, access controls, identity management etc.), periodic evaluation and monitoring of cyber-security controls, incident response, business continuity and recovery planning” (Crisanto & Prenio, 2017).

Organizations should establish were to deploy their resources, considering that they are limited and the need to maximize their benefits. Normally, legal and regulatory requirements relating data protection are starting points for the identification of critical information assets (Crisanto & Prenio, 2017).

Cyber-security is less about the technology and more about the people. Companies have been too focused in technological solutions for cyber-risk, leaving behind the ones that involve people and processes. It’s critical that companies have employees that understand the technical details of cyber-risk, but more so employees that know how to communicate cyber/risk information to the board and to the rest of the staff in a language that they understand (financial rather than technical), encouraging questions and discussions related to the topic. Also, raising cyber-security awareness among staff is essential, they need to understand the value of the assets they use every day and learn to interact with the company’s technology environment responsibly (Crisanto & Prenio, 2017).

Recent high-profile cyber-attacks have reminded us that there is a need for strengthening cyber-security and making cyber-risk a major concern. However, only a handful of jurisdictions have specific regulatory and supervisory initiatives on financial institution’s cyber-risk. These include Hong Kong SAR, Singapore, United Kingdom and United States. Collaboration between industry entities is essential to strengthen cyber-security, to pursue greater cross-border cooperation and harmonization of practices. Regulators should work closely with the industry, creating and promoting sharing spaces where cyber-security professionals help each other. This could be very helpful for jurisdictions with limited regulatory and supervisory resources and smaller institutions (Crisanto & Prenio, 2017).

Any cyber-security framework should be aligned with the overall operational risk and enterprise-wide risk management strategy. Given that an effective cyber-attack is very likely to affect people, processes and technology, it would be very challenging, if cybersecurity is managed by itself, with its own set of responsibilities, policies and procedures within IT, without taking into account the operational risk management framework and the entire company. To mitigate this challenge, cyber/risk needs to be incorporated in the organizations overall risk management framework and governance structure (ISO/IEC 2018, 2018), having an advanced planning, cooperation and communication between the operational, risk, infrastructure and cyber-security areas. Like any other risk, cyber-risk should be subject to the general risk management principles of risk identification, control, monitoring and mitigation; and if necessary additional guidelines may be issued applying or clarifying the application of the general risk management regulations to cyber-risk (Crisanto & Prenio, 2017).

Enterprises have to view cyber security breaches as a risk, with their associated probabilities and impacts; increasing their own resilience and protection. However,

they have to be aware that despite their best efforts it’s not likely to completely avoid security issues in the digitally-connected world (Accenture, 2016b).

Cyber-attacks can be considered as a part of operational risk, given that the definition of operational risk according to the Basel Committee is: “The risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems, or from external events” (Bank for International Settlements, 1998).Thus, operational risk can result from cyber security breaches from external criminals or internally disgruntled employees (Accenture, 2016b). Alignment across operational risk management procedures and cyber security is essential (Accenture, 2016b).

2 METHODOLOGY

2.1 Analyze parameters and variables that make up the AHP.

Considering that Cyberrisk measurement is the application for the proposed model in terms of a case study, the main components that make up the cyber program management (CPM) have to be identified and analyzed in the first stage.

Every technological advance brings both opportunities and risks. As technology advances, the speed and severity of security threats intensifies and the information becomes more critical, making companies dependent on their information systems and the technologies that enable them.

A cyber-attack can affect the ability of an organization to fulfill its core business activity or it can threaten it operations, production capabilities, customer and/or employee data, liability exposure and intellectual property, any one of which could jeopardize business continuity and integrity (EY, 2014). Therefore, reputational damage among different stakeholder groups cannot be overstated, which proofs that cybersecurity must be an essential part of the organization's overall risk management strategy.

Organizations can benefit from an objective assessment of their information security programs and structures and how they shape and fit into the organizations overall risk management structure (EY, 2014).

CPM is a global cross-standard application, which contains a multi-level approach, since it is the framework for the people, processes and technology that an organization uses to establish, implement, operate, monitor, review, maintain and improve a security program within the context of an organization's overall business objectives and activities. Thus, it offers a rigorous risk identification and management cycle, which helps an organization anticipate new challenges from emerging technologies and business trends (EY, 2014).

CPM links security management with business performance by helping organizations align their strategic objectives through:

1. Identification of real risks
2. Protection of what matters most
3. Sustaining an enterprise program
4. Embedding security in the business

CPM assessments are of special interest to businesses that have recently experienced a public or private breach resulting in data loss, reputational damage and brand impairment. Also, it is very useful for companies, that are unsure about their current risk exposure, that they invest in cybersecurity but need to prioritize spending, that are interested in how their current capabilities compare to their colleagues, that want to validate if their security investments have improved the overall security, that need assistance assessing the maturity of their cybersecurity and identifying areas for improvement, etc. (EY, 2014).

CPM is a means to evaluate objectively any organization's security program, thus, it helps in balancing costs, risk and value. It identifies gaps in security, which helps executives in making strategic and prioritized investments; reducing costs, addressing business needs, increasing the value of the company and keeping it safe (EY, 2014).

2.2 Design a model for constructing risk matrices using the structure of an AHP model.

To develop the impact and management matrices, we apply two separate methodologies.

2.2.1 Management Matrix

The structure for the design of the management matrix mixes methods for decision making with the principles of fuzzy logic. In the first phase, the qualitative variables that make up a cyber program management will be modeled, according to the hierarchical decision tree that is defined for them. The preferences of three experts will be integrated into the model, when comparing each of the levels of the hierarchical decision tree and the resulting weights will refer to the severity, given that they represent the relative importance of each element in the decision. At the same time, five experts will answer a questionnaire referring to the frequency of the same qualitative variables that make up a cyber program management. Given the high quantity of qualitative information that these variables store, these will be modeled by using the principles of fuzzy logic (Annexe 1: Questionnaire and AHP).

2.2.1.1 Step 1: Analytic Hierarchy Process (AHP)

Analytic Hierarchy Process (AHP) is a multi-criteria decision-making approach, introduced by Saaty in the year 1980 (Sadhana & Shanmugapriya, 2017). Its main characteristics are mathematical sustenance, impartiality, management of quantitative and qualitative criteria, and its system of logical comparisons. AHP allows a problem to be analyzed by parts, by decomposing a decision process into its constituent elements (subproblems) in order to make them easier to comprehend. This method has been widely used worldwide due to its flexibility when mixing it with optimization methods and for allowing to incorporate the knowledge that exists in the human brain when making decisions based on preferences (Wind & Saaty, 1980).

The method consists in constructing a hierarchical tree based on levels for the qualification of alternatives, assessing the relative importance of decision criteria. The first level corresponds to the criteria taken into account to make a decision. The following levels contain the sub-criteria that describe each of the criteria that are in the previous level of the hierarchical tree. So, the second level is composed by the sub-criteria that describes each of the criteria of the first level and they play the role of the criteria for the third level. For the constructed hierarchical tree, the method uses comparison matrices to store the preferences of an expert for each level of criteria, thus determining an overall priority for each decision alternative and an overall ranking for the decision alternatives in the decision making process (Wind & Saaty, 1980).

First, the hierarchical decision tree (*HDT)* must be built. At the top of the tree the desired objective is located for which a decision is required; the first level is composed by the main criteria fundamental to make the decision, and the lower levels by the sub-criteria that describes each higher-level criterion. Each level of the hierarchical tree must have at least three elements. In Figure 4 you can see a hierarchical decision tree which has n first-level criteria, criterion 1 ($C1$) is described by $nsc1$ (number of sub-criteria for criterion 1) sub-criteria, criterion 2 ($C2$) has no sub-criteria and the criterion n (Cn) is described by $nscn$ (number of sub-criteria for criterion n) sub-criteria. This hierarchical tree only has two levels; however, more levels can be deployed from the second level. The number of levels must be chosen according to the description of the problem (Mu & Pereyra-Rojas, 2017).

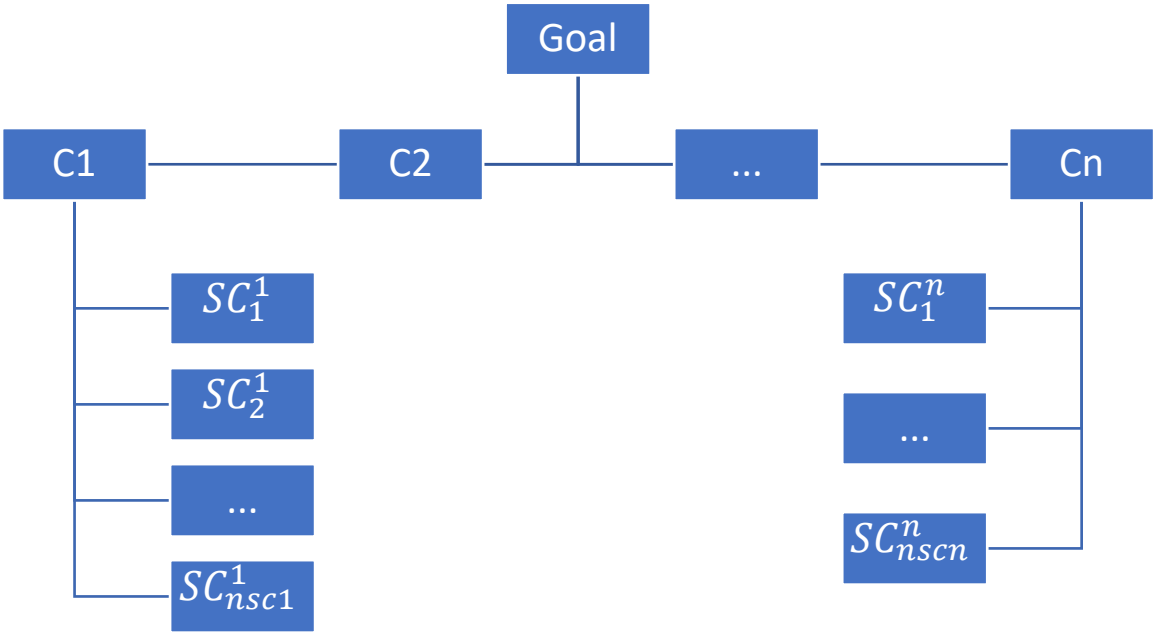


Figure 4: Hierarchical Decision Tree
Created by author.

After decomposing the problem into a hierarchical structure, that shows the relationship between goals, criteria and sub-criteria or alternatives, involved in the decision process, the comparison matrices ($CMnxn$) must be built for each level of the hierarchical decision tree. These matrices consist in comparing each group of criteria of a level of *HDT* with themselves, assigning to each position of the matrix a preference value of one criterion over the other. The assigned preference values are taken from the scale of values proposed by Saaty (see Figure 5); for example, when buying a car a person can consider that cost is very strongly more important than the comfort factor, thus the cost-comfort comparison cell will contain the value 7. The main diagonal of these matrices has the value of one, implying that there is no preference between equal criteria, and the symmetrical elements, with respect to the diagonal, meet the equality of Equation (1) (Mu & Pereyra-Rojas, 2017).

$$a_{ij} = \frac{1}{a_{ij}}, \qquad where\ i\ represents\ the\ row\ and\ j\ the\ column \tag{1}$$

AHP scale for combinations.

Numerical scale	Definition	Verbal explanation
1	Equal significance of the two elements	Two elements contribute equally to the property
3	Low significance of one element compared to another	Experience and personal assessments favor one element slightly over another
5	Strong significance of one element compared to another	Experience and personal assessments favor one element strongly over another
7	Confirmed dominance of one element over another	One element is strongly favored and its dominance is borne out in practice
9	Absolute dominance of one element over another	The evidence favoring one element over another appears irrefutable
2, 4, 6, and 8	Intermediate values between two neighboring levels	The assessment falls between two levels
Reciprocals (1/x)	A value attributed when activity *i* is compared to activity *j* becomes the reciprocal when *j* is compared to *i*	

Figure 5: AHP scale for combinations
Retrieved from: (Aminbakhsh et al., 2013).

Table 1 below shows the comparison matrix for the criteria of level 1 and the comparison matrix for level 2 for the sub-criteria that make up criterion 1.

Table 1: Comparison Matrix

Level 1	C_1	C_2	…	C_n
C_1	1	a_{12}	…	a_{1n}
C_2	a_{21}	1	…	a_{2n}
…	…	…	…	…
C_n	a_{n1}	a_{n2}	…	1

Level 2 C_1	SC_1	SC_2	…	SC_n
SC_1	1	a_{12}	…	a_{1nsc}
SC_2	a_{21}	1	…	a_{2nsc}
…	…	…	…	…
SC_n	a_{nsc1}	a_{nsc2}	…	1

Created by the author.

Then, because the comparison matrix has a very low inconsistency, the approximate method will be used due to its simplicity, for more details see the following reference. Each of the $CMnxn$ that were obtained according to the hierarchical decision tree must be normalized. For each matrix the sum of each of its columns must be calculated and then each element has to be divided by the sum of its corresponding column (see Equation *(2)*) (Mu & Pereyra-Rojas, 2017).

$$an_{ij} = \frac{a_{ij}}{\sum_{i=1}^{n} a_{ij}} \quad (2)$$

From each normalized comparison matrix ($NCMnxn$) the overall or final priorities will be obtained by calculating the averages (Pi) of the rows for each (see Equation *(3)*) (Mu & Pereyra-Rojas, 2017).

$$P_i = \frac{\sum_{j=1}^{n} an_{ij}}{n} \quad (3)$$

The sum of the averages calculated for each of the $NCMnxn$ must be one and represents the priorities or weights of importance for each of the elements that make up the matrix. Pi is a vector of size $nx1$ ($Pnx1$) that allows to evaluate each of the alternatives for decision making present in the problem.

Once judgments have been entered, it is necessary to check that they are consistent. Since the numeric values are derived from the subjective preferences of individuals, it is impossible to avoid some inconsistencies in the final matrix of judgments. The issue is, how much inconsistency is acceptable. For this purpose, AHP calculates a consistency ratio (CR) comparing the consistency index (CI) of the matrix in question (the one with our judgments) versus the consistency index of a random-like matrix (RI), where the judgments have been entered randomly and therefore it is expected to be highly inconsistent (see Equations *(4)* and *(5)*) (Mu & Pereyra-Rojas, 2017).

$$\text{Consistency ratio} = \text{CR} = \frac{\text{CI}}{\text{RI}} \quad (4)$$

$$\text{Consistency index} = \text{CI} = \frac{\lambda\text{max} - \text{n}}{\text{n} - 1} \quad (5)$$

In Equation *(5)*, n represents the number of criteria compared in the $CMnxn$ and the parameter λmax is the maximum eigenvalue of matrix D and is calculated as follows:

- Each $CMnxn$ is multiplied by the vector with the priorities or weights of importance ($Pnx1$) to find the vector $P'nx1$.
- Each position of the vector $P'nx1$ is divided by its corresponding position in the vector $Pnx1$, obtaining the vector $Dnx1$.
- λmax is calculated as the average $Dnx1$.

For the calculation of RI, Saaty approximates random indexes for different numbers of criteria n based on many trials. These can be seen in Figure 6.

Random consistency (RC) index [n = size of the reciprocal matrix].

n	1	2	3	4	5	6	7	8	9	10
RC	0	0	0.58	0.9	1.12	1.24	1.32	1.41	1.45	1.49

Figure 6: Random consistency (RC) index

Retrieved from: (Aminbakhsh et al., 2013).

Saaty (1980) has shown that a consistency ratio (CR) of 0.10 or less is acceptable to continue the AHP analysis, but if it is greater than 0.10, it is necessary to revise the judgments of the matrix, to locate the cause of the inconsistency and to correct it.

The Fuzzy Analytic Hierarchy Process (FAHP) is an advanced method of AHP, it is more effective when information is highly qualitative, because it deals with subjective judgment by applying fuzzy theory, which provides a systematic tool to deal with qualitative and quantitative data and information. So, it is used to clear the uncertainty of decision-making errors of individuals (Sadhana & Shanmugapriya, 2017).

2.2.1.2 Step 2: Questionnaire

In that same order of ideas, each sub-criterion (question) has possible answers in terms of the frequency. These answers are not part of the hierarchical structure since they are responsible for assigning a value of frequency to each sub-criterion, in such a way that a total score and a level of risk can be obtained for implementing a CPM in an organization.

Also, according to the Cyber Program Management developed by Ernst & Young Cybersecurity Advisory practice in 2014 after a meaningful analysis of how information security shapes and fits into an organization's overall risk management structure, the sub-criterions (question) for each of criterion were defined.

The quantitative component is based on the judgment or knowledge of the experts and the information reported in the media.

It was necessary to identify the alternatives for each model criterion, which resulted from a thorough bibliographical analysis and discussion. For this purpose, each sub-criterion was classified as qualitative or quantitative, according to the nature of the information referred to.

Given that the answer to a quantitative sub-criterion is a numerical value, it can be deduced that all the sub-criteria are quantitative. For this type of sub-criterion, each of the five experts answered with a number from 1 to 5, taking into account that:

- 1 refers to Rare;
- 2 refers to Unlikely;
- 3 refers to Possible;
- 4 refers to Likely;
- 5 refers to Almost Certain;

2.2.1.3 Step 3: Fuzzy Sets

Fuzzy logic has gained strength in recent years thanks to its ability to represent the real world as human beings think and its ability to work under uncertainty with inaccurate information (Demirel et al., 2008). Fuzzy logic is a tool that allows to

incorporate qualitative information and expert knowledge, into systems that standardize the way in which the brain reasons (Kulak et al., 2005).

Each of the experts has different criteria when responding, so the answers differ among decision makers. This difference gives rise to inaccurate information for decision making and makes it necessary to use concepts such as fuzzy logic, which allows to work with this type of information and to mix qualitative variables with quantitative ones.

In fuzzy logic, we speak of sets, to which an element can belong with a certain degree of truth. This characteristic makes makes it different compared to the classical logic, in which an element does belong or does not belong to a set in its entirety. These sets are known as fuzzy sets, and the truth-value of the membership of an element in a set is given by a mathematical function known as a membership function.

There is no general rule or formula to determine the number of fuzzy sets that should be used in the construction of risk levels. Del Brío & Sanz Molina (2005) recommend using a number of odd fuzzy sets. They also mention that a value of less than three fuzzy sets does not sufficiently describe the variable that provides the information, while a number of fuzzy sets greater than seven does not provides more information about the variable that is being described.

A fuzzy set is defined by a membership function that represents the degree of truth in a cero to one interval. This means that the output must be within the interval mentioned before. A triangular membership function was used for the construction of the fuzzy sets.

A triangular fuzzy set (TFS (a, b, c)) is defined by a membership function, which in turn is defined by three points: a (lower boundary), b (center) and c (upper boundary). This function takes values greater than zero in the interval between a and c, and takes the value of one at point b, see equation (6) below.

$$u(x) = \begin{cases} 0, & x < a \\ \dfrac{x-a}{b-a}, & a \le x \le b \\ \dfrac{c-x}{c-b}, & b \le x \le c \\ 0, & x > c \end{cases} \tag{6}$$

Figure 7 shows the graph of a triangular fuzzy set.

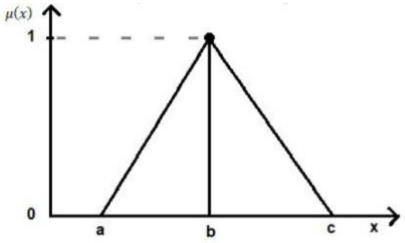


Figure 7: Triangular fuzzy Set

Created by the author

According to the classification of each sub-criterion, a methodology was proposed to unify the knowledge of the experts and to be able to construct a triangular fuzzy set that allows assigning a single level of risk and a single score to each quadrant of the matrix.

The weights obtained from the AHP process and the average of the results of the five experts to each of the 17 questions are used to obtain five fuzzy sets. First, both results are ordered from the smallest to the largest value. Then, the difference between them is calculated and divided by five, obtaining how long each interval is. Finally, the difference is summed to the smallest number. Then, the difference is summed to this result and so on. The six numbers that are acquired in this process represent the values on the x-axis that compose the five fuzzy sets. Whereas, on the y-axis the values range from 0 to 1.

After the construction of five fuzzy sets, from both frequency and severity, the average was calculated, adding all the data points located in each fuzzy set and dividing that by the number of data points added.

Finally, taking into account that the outcome must be a management matrix of 5x5 with five levels of risk and where frequency represents the y-axis and severity the x-axis. The frequency and severity are multiplied in their corresponding quadrant or position within the matrix (see `Table 2`).

Table 2: Matrix quadrants

$F_5 * S_1$	$F_5 * S_2$	$F_5 * S_3$	$F_5 * S_4$	$F_5 * S_5$
$F_4 * S_1$	$F_4 * S_2$	$F_4 * S_3$	$F_4 * S_4$	$F_4 * S_5$
$F_3 * S_1$	$F_3 * S_2$	$F_3 * S_3$	$F_3 * S_4$	$F_3 * S_5$
$F_2 * S_1$	$F_2 * S_2$	$F_2 * S_3$	$F_2 * S_4$	$F_2 * S_5$
$F_1 * S_1$	$F_1 * S_2$	$F_1 * S_3$	$F_1 * S_4$	$F_1 * S_5$

Created by the author.

2.3 Develop the proposed model through the use of dot net technologies and interoperable Microsoft Excel functions.

2.3.1 Impact Matrix

To develop the impact matrix a database of a public financial corporation was used to attain the severity and frequency, which allowed to calculate the LDA. Next, the k means of the three distributions were deduced using R, partitioning a given dataset, each distribution with 701 data points (registers) into a specific number of clusters, in this case 5.

The database contained the daily transactions, carried out at the ATMs of the financial institution, their value, the failed transactions and the respective costs generated. The database is composed of 701 daily transactions because the sample represented two

years of 365 days minus 30 days of vacation, 15 days of vacation per year (see sheet 1 of Annexe 2: Technological failures).

2.3.1.1 Step 1: K Means Clustering

Cluster analysis plays an important role in a wide variety of areas, such as business intelligence, psychology and social science (Wu, 2012). Clustering is mainly used for exploratory data mining, but it is also used in many fields, such as machine learning, pattern recognition, image analysis, information retrieval, bio-informatics, data compression, and computer graphics (Wu, 2012).

There are four important algorithms for cluster analysis, such as connectivity-based clustering, centroid-based clustering, distribution-based clustering and density-based clustering (Estivill-Castro, 2002). However, this work will only focus in the centroid-based clustering or k-means clustering.

K-means Clustering is one of the oldest and most popular clustering algorithms (Wu, 2012). It is an unsupervised learning algorithm that tries to cluster data based on their similarity (Mitchell, 1997). Unsupervised learning models are trained using data that consists only of input vectors, with no specific target output in mind (Awad & Khanna, 2015). Whereas, similarity or closeness is an amount that reflects the strength of relationship between two data objects. In k-means the default measure of closeness is the Euclidean distance (Ramakrishnan, 2009).

In k-means clustering the data will be grouped into a specify the number of clusters. The R Studio algorithm randomly assigns each observation to a cluster, forming *k* clusters with *n objects* (Al-Augby, Majewski, Majewska, & Nermend, 2014).

- Step 1: Choose the number of *k* clusters. Generally different k should be tested to realize which is the best, but in this case k will be 5 because we want a 5x5 matrix.
- Step 2: Assign each data to the closest centroid, based on the Euclidean distance between the object and the centroid. Each collection of observations assigned to a centroid is a cluster, so it results in *k* groups with *n* observations.
- Step 3: Update the centroid of each cluster based on the data assigned to each cluster. Each cluster representative is relocated to the center (arithmetic mean) of all data points assigned to it. This step is based on the observation that, given a set of points, the single best representative for this set (in the sense of minimizing the sum of the squared Euclidean distances between each point and the representative) is nothing but the mean of the data points. This is also why the cluster representative is often mentioned to as the cluster mean or cluster centroid (Ramakrishnan, 2009).
- Step 4: Minimize the distance between the data points and their respective cluster centroids, in other words minimize the total within-cluster sum of squares (WCSS), see (equations *(7)* and (*8*)). Thus, observations will move from one group to another

- Repeat steps 2 and 3 until the within cluster variation cannot be reduced any further, until no observation changes cluster or until the centroids remain the same.

(Al-Augby et al., 2014)

The standard algorithm is the Hartigan-Wong algorithm (1979), which defines the total within-cluster variation as the sum of squared distances, Euclidean distances between each observation and its corresponding centroid:

$$W(C_k) = \sum_{x_i \in C_k} (x_i - u_k)^2 \quad (7)$$

Where:

- x_i is a data point belonging to the cluster C_k
- μ_k is the mean value of the points assigned to the cluster C_k or cluster centroid

Each observation (x_i) is assigned to a given cluster such that the sum of squares (SS) distance of the observation to their assigned cluster centers (μ_k) is minimized.

The total within-cluster variation is defined in equation (8) below.

$$\text{tot. withiness} = \sum_{k=1}^{k} \mathrm{W}(C_k) = \sum_{k=1}^{k} \sum_{x_i \in C_k} (x_i - u_k)^2 \quad (8)$$

The *total within-cluster sum of square* has to be as small as possible.

2.3.1.2 Computational Intelligence Toolbox

The CIToolbox Software is a platform used to support decision making in different areas of knowledge such as: risk, identification of dynamic systems, forecasting and forecasting of financial time series. So, it models any of the areas mentioned before based on the principles of computational intelligence.

Computational Intelligence is a branch of computer science that addresses complex problems for which the traditional methodologies and approaches are ineffective. It is a wide field encompassed by mainly neuronal networks, fuzzy logic and evolutionary computation (Duch, 2007). Fuzzy logic enables the software to understand natural language, artificial neural networks allow the system to learn experiential data by operating like a biological one, and evolutionary computing helps dealing with uncertainty and imprecision by being founded on the process of natural selection, the learning theory, and probabilistic methods (Siddique & Adeli, 2013).

The computational intelligence toolbox offers a set theoretic approach to solving many types of problems where the discovery of similar perceptual granules and clusters of

perceptual objects is important. Fuzzy sets are the most common mathematical tools in typical computational intelligence frameworks (Peters, 2009).

The independent module of the CIToolbox Software allows the construction and analysis of fuzzy systems taking into account two input linguistic variables and one output linguistic variable, which can be configured in terms of the type and quantity of fuzzy sets (Peña, Lochmuller, & Patiño, n.d.).

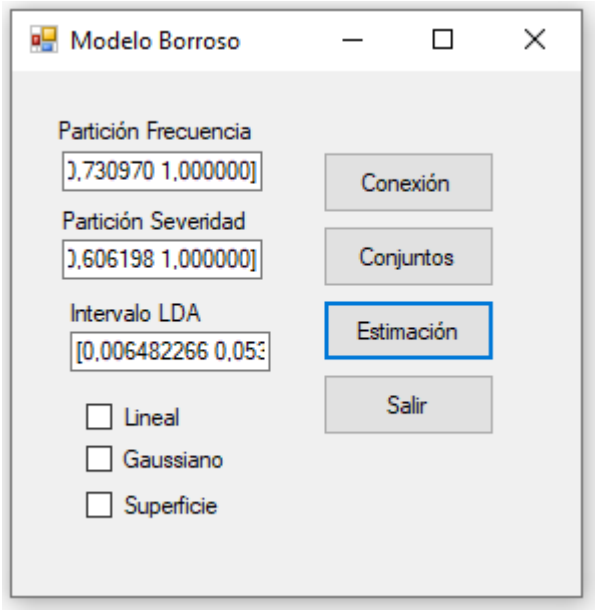


Figure 8: Structure of the main panel of the fuzzy logic model
Created by the author.

The following steps describe the procedure for using the fuzzy logic module, taking into account the main panel shown in Figure 8.

1. Press the connection button, in order to load the workspace of the module. This workspace is defined by an Excel file, Annexe 3: Fuzzy System.

2. After loading the workspace, we proceed with the configuration of the fuzzy sets that describe each of the variables. These fuzzy sets can be obtained from the data by using different clustering or grouping methods. The structure below shows how the fuzzy sets must be typed in.

$$[CL1\ CL2\ \dots\ CLn]$$

$CL1$: Represents the representative value of each fuzzy set. In the event in which the fuzzy sets are defined, in terms of Gaussian functions, these values are known as centroids.

3. To build the fuzzy sets, press the button sets (conjuntos), which will take the user to Sheet 3 (Fuzzy Sets) of Annexe 4: Fuzzy System. When pressing this

button the system will ask the user the number of fuzzy sets or qualities that the output variable will have.

Note: When the size of the interval that defines the output variable is unknown, it will be partitioned on a regular basis.

4. After finishing the configuration of the fuzzy sets, Sheet 2 (Decision-maker) must be configurated. There, each quality associated with each linguistic variable is represented numerically by a qualitative order, increasing or decreasing as follows.

Example:
0: Very Low, 1: Low, 2: Medium, 2: High, 4: Very High

The qualities associated with each of the variables should always start at zero, as shown in the previous example.

After configuring the fuzzy sets and the decision maker, we will proceed with the estimation of the output values according to the input data that allowed to define the fuzzy sets associated with each of the input linguistic variables. For the estimation process continue with the following procedure:

5. To continue with the estimation process, the user must be positioned on Sheet 1 (Estimation) of Annexe 5: Fuzzy System. .

6. In columns B and C in Sheet 1 (Estimation) of Annexe 6: Fuzzy System., the user places the pairs of values of the input linguistic variables that you want to evaluate.

Note: To ensure that the information is saved in the workspace, the Excel file must be closed, and then the connection must be opened again.

7. Before proceeding with the estimation of the output values, it is necessary to select the type of fuzzy sets that define each of the linguistic variables, Linear or Gaussian.

Note:

- If the user forgets to select the type of fuzzy sets, the default system will use the linear type for the estimation the fuzzy sets.
- For the construction of the response surface, it is necessary for the user to select the checkbox Surface. The surface allows three-dimensional visualization of the blurred functional relationship between the input and output variables, according to the decision maker that describes the management that must be done with respect to this risk.

(Peña, Lochmuller, & Patiño, n.d.)

2.4 Validate the model taking into account the behavior of the aggregated distribution of losses and the coverage percentage over the expected

losses

2.4.1 Fit probability distribution to data - MATLAB

To validate the model, it is necessary to determine the distribution of each set of data; the original frequency, the original severity, the original LDA, the LDA_1, the LDA_2, the LDA_3 and the LDA_4.

For this purpose, the ALLFITDIST function in Matlab is used. This function tries all distributions available (continuous or discrete depending on the data but continuous by default), chooses the one with the highest likelihood, returns its parameters with 95% CI (confidence interval) and plots the data and the fitting (The MathWorks, 2019a).

The ALLFITDIST(...,'PDF') or (...,'CDF') plots either the Cumulative Distribution Function (CDF) or Probability Density Function (PDF) of a subset of the fitted distribution. The distributions are plotted in order of fit, according to SORTBY. Thus, the function returns a list of valid distributions sorted by:

- NLogL: Negative of the log likelihood.
- BIC: Bayesian information criterion.
- AIC: Akaike information criterion.
- AICc: AIC with a correction for finite sample sizes.

The AICc and BIC are based on NLogL, however the AIC can be derived from the BIC approximation to the Bayes factor (Ahmed, 2018).
The Negative of the log likelihood (NLogL), the Akaike information criterion (AIC), the corrected Akaike's Information Criterion (AICc) and the Bayesian Information Criterion (BIC) are information-based criteria that assess model fit. Thus they provide a means for model selection. The distribution with the smallest value is usually the preferred model (Ahmed, 2018).

They are estimators of the relative quality of statistical models for a given set of data. Given a collection of models for the data, they estimate the quality of each model, relative to each of the other models (Ahmed, 2018).

When a statistical model is used to represent the process that generated the data, the representation will almost never be exact; so, some information will be lost by using the model to represent the process. AIC estimates the relative amount of information lost by a given model; the less information a model loses, the higher the quality of that model. In estimating the amount of information lost by a model, AIC deals with the trade-off between the goodness of fit of the model and the simplicity of the model. In other words, AIC deals with both the risk of overfitting and the risk of underfitting. Thus, when the sample size is small, there is a substantial probability that AIC will select models, which have too many parameters, that AIC will overfit. To address this problem AICc was developed, considering that AICc is AIC with a correction for small sample sizes (Ahmed, 2018).

Below is a list of distributions the ALLFITDIST function will try to fit (The MathWorks, 2019a).

Continuous (default):

- Beta
- Birnbaum-Saunders
- Exponential
- Extreme value
- Gamma
- Generalized extreme value
- Generalized Pareto
- Inverse Gaussian
- Logistic
- Log-logistic
- Lognormal
- Nakagami
- Normal
- Rayleigh
- Rician
- t location-scale
- Weibull

Discrete ('DISCRETE'):

- Binomial
- Negative binomial
- Poisson

(The MathWorks, 2019a)

2.4.1.1 Frequency Distributions

The frequency is described by discrete distributions. “The most commonly used frequency distributions for the annual number of events N are Poisson, Binomial, and Negative Binomial distributions” (Cruz et al., 2015).

- If $\mu = \sigma^2$ the data is distributed as a Poisson, because the Poisson mean equals its variance
- If $\mu > \sigma^2$ the data is distributed as a Binomial, because a Binomial’s variance is less than its mean.
- If $\mu < \sigma^2$ the data is distributed as a negative Binomial, because the variance of the Negative Binomial is larger than its mean.

(Cruz et al., 2015)

The Results from the 2008 Loss Data Collection Exercise for Operational Risk made by the Bank for International Settlements show that among 42 AMA banks participating in the questionnaire, 93% use the Poisson distribution, 19% use the Negative Binomial, and 7% use other distributions to model frequency (Basel Committee on Banking Supervision, 2009).

2.4.1.2 Severity Distributions

The severity is described by continuous distributions. The most common distributions to adjust to the severity are: LogNormal, Gamma, Weibull, Pareto, and Generalized Pareto models (Cruz et al., 2015).

The Results from the 2008 Loss Data Collection Exercise for Operational Risk made by the Bank for International Settlements show that among 42 AMA banks participating in the questionnaire

• About 31% banks apply a single severity distribution to model body and tail, with LogNormal (33%) and Weibull (17%) as the most widely used ones;

• About 30% of banks use two distributions for body and tail: LogNormal (19%) and empirical (26%) for modeling the body and LogNormal (14%) and generalized Pareto (31%) for estimating the tail;

• Other distributions used for modeling severity include Gamma, g-and-h, generalized Beta, mixture of LogNormals.

(Basel Committee on Banking Supervision, 2009)

2.4.2 LDA Distribution Model using the Distribution Fitter App - MATLAB

Subsequently, the four LDA distributions will be modeled using the distribution fitter app in Matlab. For this we follow the following procedure.

1. Enter distributionfitter at the command prompt.
2. Import the sample data (see Figure 9).

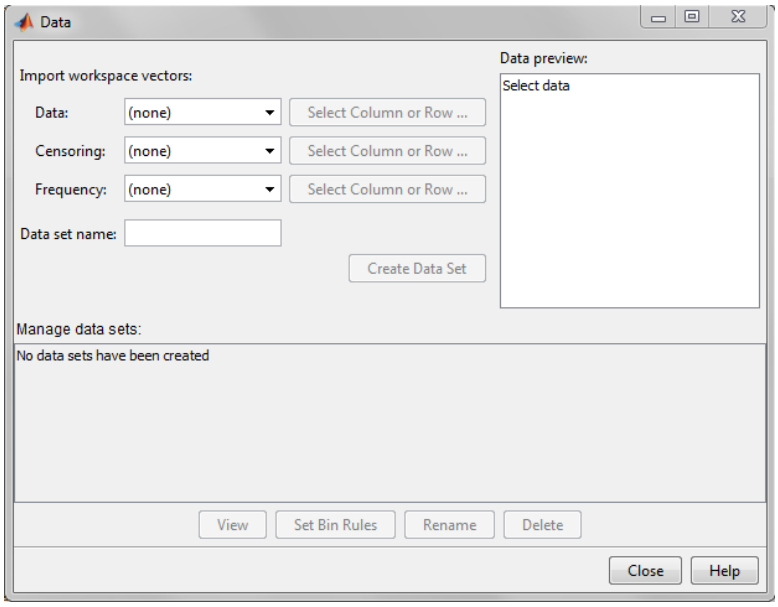


Figure 9: Data dialog box
Retrieved from: (The mathworks, 2019b).

Create a data set by importing a vector from MATLAB. First open the Data dialog box, the Data field contains a drop-down list with the names of all matrices and vectors. Select the array containing the data that we want to fit (LDA_1, LDA_2, LDA_3 and LDA_4) (*The mathworks, 2019b*).

Then, view and manage the data sets using the Manage data sets pane shown in Figure 10.

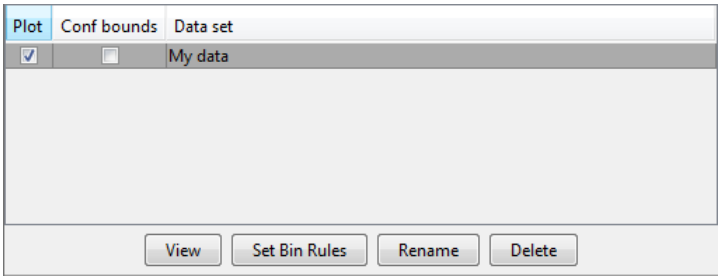


Figure 10: Manage data set pane
Retrieved from: (The mathworks, 2019b).

For each data set in the Data sets list, we can:

- Select the Plot check box to display a plot of the data in the main Distribution Fitter app window *(The mathworks, 2019b)*.
- Once the Plot is selected, we can also select Bounds to display confidence interval bounds for the plot in the main window. The bounds are displayed only when we set Display Type in the main window to one of the following:
    - Cumulative probability (CDF)
    - Survivor function
    - Cumulative hazard

  (The mathworks, 2019b)
- The Distribution Fitter app cannot display confidence bounds on density (PDF), quantile (inverse CDF), or probability plots. Clearing the Bounds check box removes the confidence bounds from the plot in the main window *(The mathworks, 2019b)*.
- When we select a data set from the list, we can also access the Set Bin Rules button. This defines the histogram bins used in the density (PDF) plot *(The mathworks, 2019b)*.
    - In this case, we left the Freedman-Diaconis rule, which is the default because it is suitable for many kinds of data and it chooses bin widths and locations automatically, based on the sample size and the spread of the data (see Figure 11) *(The mathworks, 2019b)*.

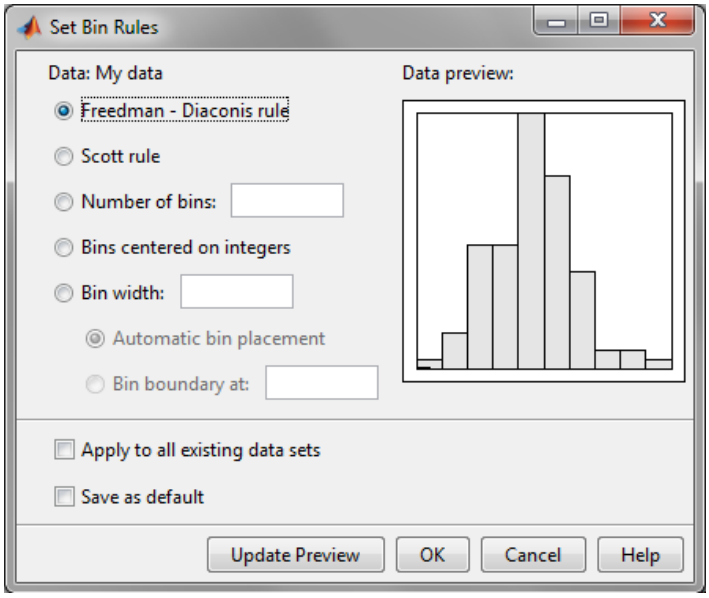


Figure 11: Set bin rules
Retrieved from: (The mathworks, 2019b).

3. Create a new fit for the data

To create a new fit for the data, click the New Fit button at the top of the main window to open the New Fit dialog box shown in Figure 12. The data set created will appear in the Data field (LDA_1, LDA_2, LDA_3 and LDA_4) *(The mathworks, 2019b)*.

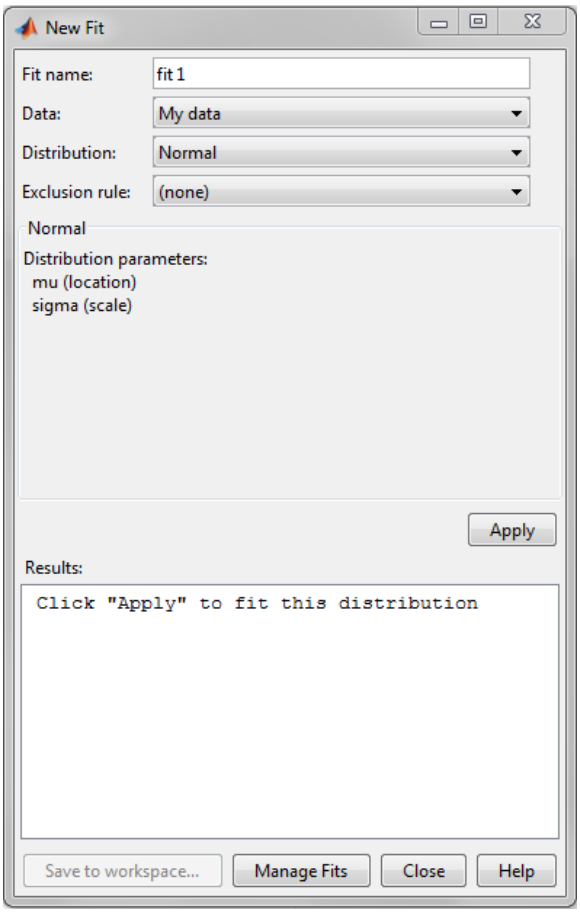


Figure 12: New fit dialog box

Retrieved from: (The mathworks, 2019b).

- In the dialogue box of the Fit Name enter a name for the fit *(The mathworks, 2019b)*.
- In the dialogue box of the data, select the data set to which we want to fit a distribution from the drop-down list (The MathWorks, 2019b).
- In the dialogue box of the distribution, select the type of distribution to fit from the Distribution drop-down list (The MathWorks, 2019b).

    - Only the distributions that apply to the values of the selected data set appear in the Distribution field. For example, when the data include values that are zero or negative, positive distributions are not displayed (The MathWorks, 2019b).

4. Display the results of the fit as a density (pdf), a cumulative probability (cdf), a quantile (inverse cdf), a probability plot (choose one of several distributions), a survivor function, or a cumulative hazard (The MathWorks, 2019b).

In this case, we will choose the Density (PDF) that displays a probability density function (PDF) plot for the fitted distributions (LDA_1, LDA_2, LDA_3 and LDA_4). The main window displays data sets using a probability histogram, in which the height of each rectangle is the fraction of data points that lie in the bin divided by the width of the bin. This makes the sum of the areas of the rectangles equal to 1 (The MathWorks, 2019b).

By modeling the data, we want to confirm that as the management becomes stronger the heavy tailed aggregated loss distribution will become slenderer, consequently the probability of catastrophic events happening decreases. Also, that the LDA distributions keep the structure and form of fat tailed probability distributions representative of this type of risk such as: Weibull, Lognormal, Loglogistic or Generalized Pareto (structural stability) (Mora & Gudiño, 2010).

The distributions that best fit the operating loss events are those with heavy tails (Mora & Gudiño, 2010). A heavy or fat tailed distribution is a probability distribution that exhibits a large skewness or kurtosis, relative to that of either a normal distribution or an exponential; in other words, has a heavier tail than an exponential distribution. More precisely, a distribution that is heavy tailed goes to zero slower than a light-tailed one, there will be more bulk under the curve of the Probability Distribution Function (PDF).

3 PRESENTATION AND DISCUSSION OF RESULTS

3.1 Analyze parameters and variables that make up the AHP.

3.1.1 AHP model for cybersecurity

To connect the security strategy to the business performance, the approach developed by Ernst and Young Cybersecurity Advisory practice in 2014 was used. It is referred to, as the cyber program management, in which an organization has to identify real risks, protect what matters most, sustain an enterprise program and embed security into the business. These four elements are considered the main criterion for decision making in each of the developed models. Each of these criterions is composed of sub criterions that represent the variables for the construction of the models and are described in terms of questions that request information regarding the definition of the criteria. The number of sub-criterions depends of each criterion, in this case they were defined by EY.

Each sub-criterion can be quantitative or qualitative, this does not depend on the nature of the main criterion, which in turn can also be quantitative or qualitative, as mentioned above. That is to say, if the criterion is quantitative, its sub-criteria can be quantitative or qualitative, and if the criterion is qualitative, its sub-criteria can also be quantitative or qualitative.

The subcriterion-criterion relationship creates a hierarchical structure that allows modular management of the importance of each of the elements that influence decision-making when implementing a Cyber Program Management. In *Figure 13* you can see the four goals an organization has to achieve to align security management to business performance and to objectively evaluate an organization’s security program.

By structuring the problem in this way, it is possible to better understand the decision to be achieved, the criteria to be used and the alternatives to be evaluated. This step is crucial, and it is where the participation of experts is requested to ensure that all criteria and possible alternatives have been considered.

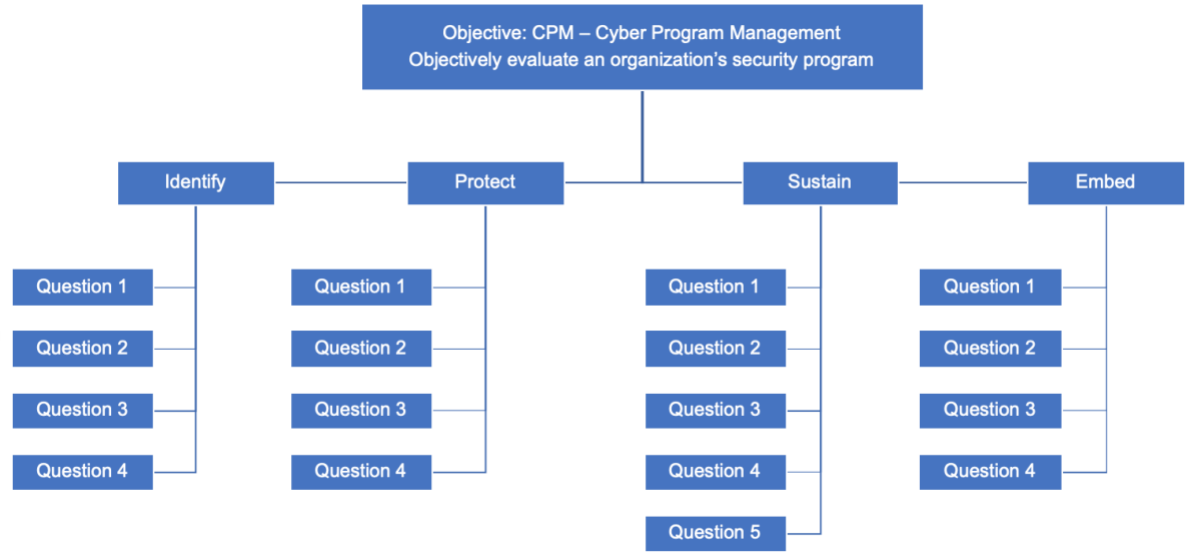


Figure 13: Hierarchical structure for the CPM
Created by the author.

Identify

- Question 1: Does the organization develop a security strategy focused on business drivers and protecting high-value data?
- Question 2: Does the organization define its overall risk appetite?
- Question 3: Does the organization identify the most important information and applications (where they reside and who has/needs access)?
- Question 4: Does the organization assess the threat landscape and develop models highlighting real exposures?
  (EY, 2014)

Protect

- Question 1: Does the organization assume breaches will occur, improve processes that complicate, detect and respond?
- Question 2: Does the organization balance the fundamentals through emerging threats and vulnerability management?
- Question 3: Does the organization establish and rationalize access control models for applications and information?
- Question 4: Does the organization protect key identities and roles because they have access to the “crown jewels”?
  (EY, 2014)

Sustain

- Question 1: Does the organization get governance right, make security a board-level priority?
- Question 2: Does the organization allow good security to drive compliance and not vice versa?
- Question 3: Does the organization measure leading indicators to catch problems while they are still small?
- Question 4: Does the organization accept manageable risks that improve performance?

- Question 5: Does the organization know its weaknesses and address them? (EY, 2014)

Embed

- Question 1: Does the organization make security everyone's responsibility (it is a business problem, not just an IT problem)?
- Question 2: Does the organization align all aspects of security (information, privacy, physical and business continuity) with the business?
- Question 3: Does the organization spend wisely on controls and technology, invest more in people and process?
- Question 4: Does the organization selectively consider outsourcing or co-sourcing operational security program areas?
  (EY, 2014)

3.2 Design a model for constructing risk matrices using the structure of an AHP model.

From the hierarchical decision tree, the comparison matrices were developed. For the proposed structure, it is necessary to build five comparison matrices, one to compare the five first-level criteria and one for each set of second-level sub-criteria *(*Annexe 1: Questionnaire and AHP*)*.

Error! Reference source not found. shows the comparison matrix of the criteria involved in the decision.

Criteria	Indentify	Protect	Sustain	Embed
Indentify	1,00	5,00	1,00	0,33
Protect	0,20	1,00	0,33	0,20
Sustain	1,00	3,00	1,00	1,00
Embed	3,00	5,00	1,00	1,00
SUM	**5,20**	**14,00**	**3,33**	**2,53**

Figure 14: Pairwise comparison matrix of criteria
Created by the author.

The numeric scale shown in Figure 5 reflects the relative preference or judgement of the expert. For example, the expert considered that identify is strongly more important than protect. This is why the identify-protect comparison cell has a value of 5. Mathematically this means that the ratio of the importance of identify versus the importance of protect is five (identify/protect = 5). Because of this, the opposite comparison, the importance of protect relative to the importance of identify, will return the reciprocal value (protect/identify = 1/5) as shown in the protect- identify cell in the comparison matrix in **Error! Reference source not found.**.

Also, **Error! Reference source not found.** shows that when the importance of a criterion is compared with itself; for example, identify versus identify, protect versus protect, sustain versus sustain or embed versus embed; the input value is 1 which corresponds to the intensity of equal importance in the scale of Figure 5. This makes

sense because the ratio of the importance of a given criterion with respect to the importance of itself will always be equal.

Then, the overall priorities or weights of the criteria were calculated. Because the comparison matrix has a very low inconsistency, the approximate method was used due to its simplicity. It requires the normalization of the comparison matrix. For that the sum of each of its columns must be calculated and then each element has to be divided by the sum of its corresponding column. For example, we normalized the comparison matrix of criteria by dividing 1 by 5.2, 5 by 14, 1 by 3.3, 0.33 by 2.53 and so on (see *Figure 15*).

Normalized	Indentify	Protect	Sustain	Embed
Indentify	0,192	0,357	0,300	0,132
Protect	0,038	0,071	0,100	0,079
Sustain	0,192	0,214	0,300	0,395
Embed	0,577	0,357	0,300	0,395
SUM	**1,000**	**1,000**	**1,000**	**1,000**

Figure 15: Normalized comparison matrix of criteria
Created by the author.

From this normalized matrix, we obtain the overall or final priorities (Figure 16) by simply calculating the average value of each row. Example, for the identify row: (0.192 + 0.375 + 0.3 + 0.132)/4 = 0.24.

According to the results shown in (Figure 16), it becomes clear that the expert gave more importance to embed (0.4), followed by sustain (0.27), identify (0.24) and lastly protect (0.07). In addition, we can interpret that embed has 40% of the overall importance of the criteria, followed by sustain with 27%, identify 24% and protect 7%, respectively.

P - Average	P'	D - Consistancy measure				
0,24525737	1,0174	4,1482				
0,07220937	0,2945	4,0781				
0,27533256	1,1444	4,1565				
0,40720069	1,7794	4,3697	N-Matrix Size	CI- Consistency Index	RI- Random Index	CR-Consistency Ratio
	λmax	4,1881	4	0,062709082	0,9	0,069676758

Figure 16: priority vector $Pnx1$, the vector $P'nx1$, the vector $Dnx1$, the value of λmax, the consistency index, the random index and the consistency ratio for comparison matrix of criteria
Created by the author.

To obtain P' we multiply each value in the first column of the comparison matrix in **Error! Reference source not found.** by the first criterion priority (P). For example (1 * 0.24, 0.2 * 0.24, 1 * 0.24, 3 * 0.24); multiply each value in the second column for the second criterion priority; continue this process for all the columns of the comparison matrix. Then, add the values in each row to obtain a set of values called weighted sum

(P'). In excel P' can be calculated using the MMULT function, which returns the matrix product of two arrays (each row of the CM and the P vector).

To obtain D (consistency measure) divide the elements of the weighted sum vector (P') by the corresponding priority of each criterion (P). Then calculate the average of D (consistency measure). This value is called λmax.

Then the consistency index is calculated as follows:

$$\text{Consistency index} = \text{CI} = \frac{\lambda\text{max} - \text{n}}{\text{n} - 1} \quad (9)$$

Therefore,

$$\text{CI} = \frac{4.2 - 4}{4 - 1} = 0.063$$

Finally, the consistency ratio is calculated as:

$$\text{Consistency ratio} = \text{CR} = \frac{\text{CI}}{\text{RI}} \quad (10)$$

Therefore,

$$\text{CR} = \frac{0.063}{0.9} = 0.07$$

CI is the consistency index calculated in the previous step with a value of 0.063. RI is the consistency index of a randomly generated comparison matrix and is shown in (Figure 6). In other words, RI is the consistency index that would be obtained, if the assigned judgment values were totally random. Since this value of 0.07 for the proportion of inconsistency CR is less than 0.10, it can be assumed that the judgments matrix is reasonably consistent and the process of decision-making using AHP can continue.

Figure 17, Figure 18, Figure 19, Figure 20 and Figure 21 show the four decision makers, the comparison matrices, the standardized comparison matrices, the priority vector $Pnx1$, the vector $P'nx1$, the vector $Dnx1$, the value of λmax, the consistency index, the random index and the consistency ratio.

Criteria	Indentify	Protect	Sustain	Embed
Indentify	1,00	5,00	1,00	0,33
Protect	0,20	1,00	0,33	0,20
Sustain	1,00	3,00	1,00	1,00
Embed	3,00	5,00	1,00	1,00
SUM	5,20	14,00	3,33	2,53

Normalized	Indentify	Protect	Sustain	Embed
Indentify	0,192	0,357	0,300	0,132
Protect	0,038	0,071	0,100	0,079
Sustain	0,192	0,214	0,300	0,395
Embed	0,577	0,357	0,300	0,395
SUM	1,000	1,000	1,000	1,000

P - Average	P'	D - Consistancy measure				
0,24525737	1,0174	4,1482				
0,07220937	0,2945	4,0781				
0,27533256	1,1444	4,1565				
0,40720069	1,7794	4,3697	N-Matrix Size	CI- Consistency Index	RI- Random Index	CR-Consistency Ratio
	λmax	4,1881	4	0,062709082	0,9	0,069676758

Figure 17: Comparison matrix for criteria
Created by the author.

Identify	Question 1	Question 2	Question 3	Question 4
Question 1	1,00	3,00	1,00	1,00
Question 2	0,33	1,00	0,33	0,33
Question 3	1,00	3,00	1,00	1,00
Question 4	1,00	3,00	1,00	1,00
SUM	3,33	10,00	3,33	3,33

Normalized	Question 1	Question 2	Question 3	Question 4
Question 1	0,300	0,300	0,300	0,300
Question 2	0,100	0,100	0,100	0,100
Question 3	0,300	0,300	0,300	0,300
Question 4	0,300	0,300	0,300	0,300
SUM	1,000	1,000	1,000	1,000

P - Average	P'	D - Consistancy measure				
0,3	1,1444	3,8147				
0,1	0,3815	3,8147				
0,3	1,1444	3,8147				
0,3	1,1444	3,8147	N-Matrix Size	CI- Consistency Index	RI- Random Index	CR-Consistency Ratio
	λmax	3,8147	4	-0,061756956	0,9	-0,068618841

Figure 18: Comparison matrix for identify
Created by the author.

Protect	Question 1	Question 2	Question 3	Question 4
Question 1	1,00	1,00	5,00	1,00
Question 2	1,00	1,00	3,00	3,00
Question 3	0,20	0,33	1,00	1,00
Question 4	1,00	0,33	1,00	1,00
SUM	3,20	2,67	10,00	6,00

Normalized	Question 1	Question 2	Question 3	Question 4
Question 1	0,313	0,375	0,500	0,167
Question 2	0,313	0,375	0,300	0,500
Question 3	0,063	0,125	0,100	0,167
Question 4	0,313	0,125	0,100	0,167
SUM	1,000	1,000	1,000	1,000

P - Average	P'	D - Consistancy measure				
0,33854167	1,4542	4,2954				
0,371875	1,5792	4,2465				
0,11354167	0,4813	4,2385				
0,17604167	0,7521	4,2722	N-Matrix Size	CI- Consistency Index	RI- Random Index	CR-Consistency Ratio
	λmax	4,2632	4	0,087717056	0,9	0,097463396

Figure 19: Comparison matrix for protect
Created by the author.

Sustain	Question 1	Question 2	Question 3	Question 4	Question 5
Question 1	1,00	1,00	0,33	0,33	0,33
Question 2	1,00	1,00	0,33	1,00	0,20
Question 3	3,00	3,00	1,00	1,00	0,33
Question 4	3,00	1,00	1,00	1,00	1,00
Question 5	3,00	5,00	3,00	1,00	1,00
SUM	11,00	11,00	5,67	4,33	2,87

Normalized	Question 1	Question 2	Question 3	Question 4	Question 5
Question 1	0,091	0,091	0,059	0,077	0,116
Question 2	0,091	0,091	0,059	0,231	0,070
Question 3	0,273	0,273	0,176	0,231	0,116
Question 4	0,273	0,091	0,176	0,231	0,349
Question 5	0,273	0,455	0,529	0,231	0,349
SUM	1,000	1,000	1,000	1,000	1,000

P - Average	P'	D - Consistancy measure	N-Matrix Size	CI- Consistency Index	RI- Random Index	CR-Consistency Ratio
0,08676877	0,4633	5,3399				
0,10823568	0,5637	5,2077				
0,21379469	1,1452	5,3564				
0,22394268	1,1735	5,2403				
0,36725819	2,0341	5,5385	5	0,084145866	1,12	0,075130237
	λmax	5,3366				

Figure 20: Comparison matrix for sustain
Created by the author.

Embed	Question 1	Question 2	Question 3	Question 4
Question 1	1,00	1,00	1,00	1,00
Question 2	1,00	1,00	0,33	0,33
Question 3	1,00	3,00	1,00	1,00
Question 4	1,00	3,00	1,00	1,00
SUM	4,00	8,00	3,33	3,33

Normalized	Question 1	Question 2	Question 3	Question 4
Question 1	0,250	0,125	0,300	0,300
Question 2	0,250	0,125	0,100	0,100
Question 3	0,250	0,375	0,300	0,300
Question 4	0,250	0,375	0,300	0,300
SUM	1,000	1,000	1,000	1,000

P - Average	P'	D - Consistancy measure	N-Matrix Size	CI- Consistency Index	RI- Random Index	CR-Consistency Ratio
0,24375	1,0000	4,1026				
0,14375	0,5450	3,7912				
0,30625	1,1444	3,7369				
0,30625	1,1444	3,7369	4	-0,052710896	0,9	-0,058567662
	λmax	3,8419				

Figure 21: Comparison matrix for embed
Created by the author.

3.2.1 Cybersecurity Questionnaire

In that same order of ideas, each sub-criterion (question) has possible answers. These answers are not part of the hierarchical structure since they are responsible for assigning a value of frequency to each sub-criterion, in such a way that a total score and a level of risk can be obtained for implementing a CPM in an organization.

The quantitative component is based on the judgment or knowledge of the experts and the information reported in the media.

Given that the answer to a quantitative sub-criterion is a numerical value, it can be deduced that all the sub-criteria are quantitative. For this type of sub-criterion, each of the experts answered with a number from 1 to 5, taking into account that:

- 1 refers to Rare;
- 2 refers to Unlikely;
- 3 refers to Possible;

- 4 refers to Likely;
- 5 refers to Almost Certain;

An example for this case is shown in Table 3, were expert one and two say the organization develops almost certainly a security strategy focused on business drivers and protecting high-value data. Whereas, expert three says it is “rare” and expert four says that it is “possible”.

Table 3 : Example of answers for a quantitative sub criterion.

Question	**Expert 1**	**Expert 2**	**Expert 3**	**Expert 4**
Does the organization develop a security strategy focused on business drivers and protecting high-value data?	5	5	1	3

Created by the author.

The complete questionnaire with all 17 questions and 4 answers on from each expert can be found in Annexe 1: Questionnaire and AHP.

3.2.2 Fuzzy Sets

Each of the experts has different criteria when responding, so the answers differ among decision makers. This difference gives rise to the appearance of inaccurate information for decision making and makes it necessary to use concepts such as fuzzy logic, which allows to work with this type of information and to mix qualitative variables with quantitative ones.

According to the classification of each sub-criterion, a methodology was proposed to unify the knowledge of the experts and to be able to construct a fuzzy set that allows assigning a single level of risk and a single score to each quadrant of the matrix (see Annexe 1: Questionnaire and AHP).

The weights obtained from the AHP process and the average of the results of the five experts to each of the 17 questions are used to obtain five fuzzy sets. First, both results are ordered from the smallest to the largest value. Then, the difference between them is calculated and divided by five, obtaining how long each interval is. Finally, the difference is summed to the smallest number. then, the difference is summed to this result and so on. The six numbers that are acquired in this process represent the values on the x-axis that compose the five fuzzy sets. Whereas on the y-axis the values range from 0 to 1. See Figure 22 for the severity and Figure 23 for the frequency.

Question	Weights (b)	Position
8	0.01340792	1
7	0.01396231	1
2	0.01892548	1
6	0.02892134	1
5	0.03531234	1
12	0.04250177	2
9	0.04278351	2
1	0.04590835	2
3	0.04699234	2
11	0.05066387	2
10	0.05634155	2
4	0.0641911	2
13	0.06843537	3
15	0.07145313	3
14	0.10708097	4
17	0.14361149	5
16	0.14950715	5

Difference	0.13609923
Intervals	0.02721985

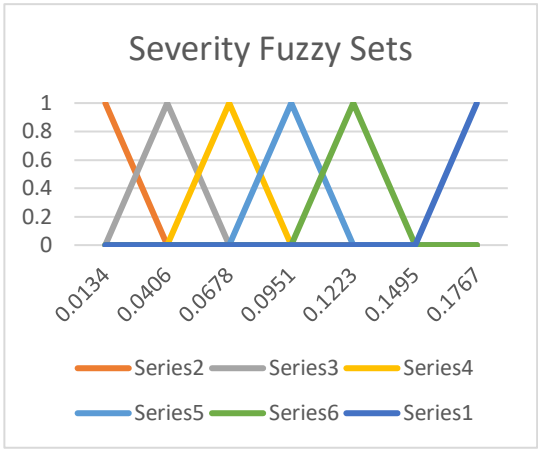


Figure 22: Severity fuzzy sets and its process
Created by the author.

Question	Questionnaire	Position
12	2	1
2	2.25	1
4	2.75	2
13	2.75	2
14	2.75	2
17	2.75	2
8	3	3
9	3	3
10	3	3
16	3	3
5	3.25	4
1	3.5	4
6	3.5	4
7	3.5	4
11	3.5	4
15	3.5	4
3	4	5

Difference	2
Intervals	0.4

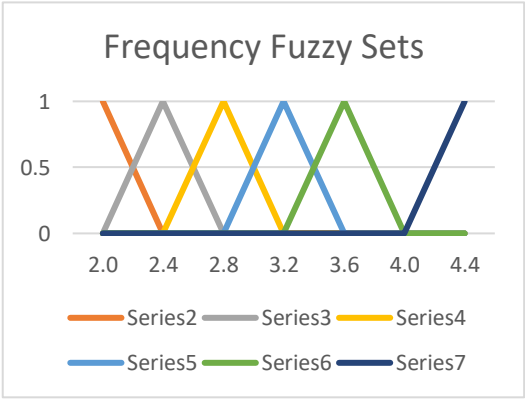


Figure 23: Frequency fuzzy sets and its process
Created by the author.

After the construction of five fuzzy sets from both, frequency and severity, the seventeen data points that where located in each fuzzy set were calculated using the COUNTIF formula in excel. Then, the average was calculated, adding all the data points located in each fuzzy set with the SUMIFS formula in excel and then dividing that by the number of data points added, found before with the COUNTIF function (see Table 4 and Table 5). For example, for the severity the sum of the data points that are positioned in fuzzy set number 1 is 0.11, and that is divided by 5 because that is the number of data points that are in that set. This results in 0.022.

Table 4: Severity Fuzzy Sets

Number of Fuzzy Sets	Number of data Points	Average
1	5	0.02210588
2	7	0.04991178
3	2	0.06994425
4	1	0.10708097
5	2	0.14655932

Created by the author.

Table 5: Frequency Fuzzy Sets

Number of Fuzzy Sets	Number of data Points	Average
1	2	2.125
2	4	2.75
3	4	3
4	6	3.46
5	1	4

Created by the author.

Finally, taking into account that the outcome must be a management matrix with five levels of risk and that frequency is shown on the y-axis and severity on the x-axis, the frequency and severity values are multiplied in their corresponding quadrant or position within the matrix (see Figure 24). For example, 0.22 (severity) is multiplied by 2.12 (frequency) resulting in 0.04, which is positioned in (x_1, y_1). We multiply these values as we assume that frequency and severity are independent variables.

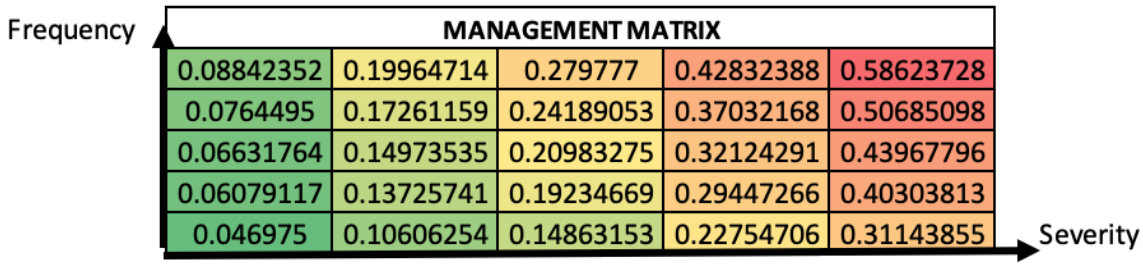


Figure 24: Management matrix
Created by the author.

3.3 Develop the proposed model through the use of dot net technologies and interoperable Microsoft Excel functions.

3.3.1 K-means Clustering

In R (R Studio) the K means algorithm (from the stats package) partitions a given dataset into a user specified number of clusters, k.

The R function used to run the k mean algorithm is:

```
kmeans(df, k)
arguments:
-df: dataset used to run the algorithm
-k: Number of clusters
```

In this case, the data sets are the number of failed transactions per day and the respective cost generated, which represent the frequency and the severity. In both situations the number of clusters is 5, given that the outcome will be an impact matrix of 5x5 with 5 levels of risk.

- Kmeans(severity,5)
- Kmeans(frequency,5)

As a result, this function sheds the cluster means, the clustering vector, the within cluster sum of squares by cluster, the between_SS / total_SS and the size of each cluster.

Below the cluster means or centroids for the severity and frequency are shown:

Severity cluster means:

1) 0.6186964
2) 1.7131577
3) 3.4040359
4) 10.5898632
5) 6.4195500

Frequency cluster means:

1) 3.990599
2) 1.336735
3) 8.806452
4) 12.047619
5) 6.360656

Below the clustering vector for the severity and frequency is shown:

Severity clustering vector:

```
  [1] 1 2 1 1 2 1 1 4 2 1 2 2 1 1 2 1 3 5 1 3 2 1 3 2 3 1 1 1 1 1 1 1
 [33] 1 1 2 3 1 1 5 1 1 2 1 1 2 1 2 1 2 1 3 1 2 1 1 3 2 1 1 1 1 3 1 1
 [65] 5 2 2 2 1 3 1 1 1 1 3 2 3 1 2 1 2 1 2 1 1 1 4 1 2 3 3 3 2 2 2 2
 [97] 2 1 4 2 1 1 2 1 2 1 1 1 5 1 2 1 2 5 5 2 2 1 3 1 1 1 3 3 1 2 3 2
[129] 1 1 1 1 5 4 1 1 1 2 2 1 1 1 1 2 2 2 2 2 1 1 1 5 1 1 2 2 3 3 2 1
[161] 1 1 2 1 3 1 1 1 3 2 3 2 2 2 1 2 2 2 1 1 1 1 1 3 1 1 1 2 1 4 1 2
[193] 5 1 3 2 2 1 3 2 1 1 4 2 1 1 3 1 2 2 2 1 1 3 2 2 5 4 4 1 3 3 1 1
[225] 1 2 2 3 5 1 3 5 2 1 2 2 1 1 5 1 1 1 1 2 1 2 3 4 3 2 5 2 4 2 2 3
[257] 1 1 3 2 1 1 2 1 2 1 1 3 2 1 2 1 2 3 1 2 2 1 1 3 1 1 3 2 1 2 5 1
```

```
[289] 1 1 3 1 3 3 2 1 2 1 4 1 2 2 1 2 1 2 4 1 1 1 1 1 2 3 1 3 1 2 1 1
[321] 2 1 1 1 1 1 1 1 3 4 1 2 1 1 2 1 2 2 2 2 1 2 1 1 2 1 1 1 2 1 1 1
[353] 1 2 2 1 1 3 3 1 1 1 2 2 3 2 1 3 1 2 1 1 1 3 2 1 5 2 1 1 4 2 1 4
[385] 2 1 2 3 3 2 3 2 1 1 1 1 2 2 3 1 2 2 2 3 2 5 1 2 1 1 4 3 5 1 1 1
[417] 4 5 1 1 3 1 1 1 2 1 1 1 1 1 2 1 1 2 1 1 1 1 2 2 1 2 1 1 3 3 2 1
[449] 3 3 1 3 1 2 5 1 2 1 1 1 1 2 1 1 1 3 2 1 3 3 2 2 3 2 2 1 1 1 1 2
[481] 1 1 2 1 2 1 2 1 1 2 2 1 1 2 3 1 2 2 5 2 1 1 2 3 2 2 1 1 2 1 1 1
[513] 3 5 1 3 3 1 1 3 3 5 1 3 3 1 2 1 1 2 3 2 2 1 1 2 2 1 1 1 1 3 1 3
[545] 2 5 1 1 1 3 5 3 1 1 1 4 3 1 2 1 1 2 3 2 5 2 1 1 2 1 2 1 5 2 2 1
[577] 1 1 3 3 1 2 1 2 1 1 2 2 3 2 3 1 1 2 2 2 1 1 2 1 1 1 2 2 1 1 1 1
[609] 2 5 2 3 5 1 4 1 2 1 1 2 2 5 1 5 1 1 2 5 2 1 2 5 2 3 2 1 3 2 1 5
[641] 2 2 2 5 3 2 1 1 3 3 3 1 1 2 2 3 5 3 1 1 2 3 1 1 1 1 2 2 1 1 2 2
[673] 1 1 1 3 3 2 2 2 2 2 3 1 1 2 1 2 3 2 2 3 3 1 2 2 1 1 1 1 1 1
```

The clustering vector tells us, to which cluster each observation belongs. For example, in the severity clustering vector observation 1 belongs to cluster 1, the observation 2 belongs to cluster 2, observation 3 belongs to cluster 1 and so on.

Frequency clustering vector:

```
  [1] 2 1 1 5 5 1 2 3 2 5 5 4 1 2 2 1 3 5 3 5 3 3 2 1 1 3 1 1 1 3 5 2
 [33] 1 3 2 1 5 3 2 1 2 5 2 3 5 5 3 4 5 3 2 2 1 2 2 5 5 5 1 1 2 3 1 3
 [65] 3 2 5 1 1 1 3 3 1 2 2 2 2 4 1 2 2 4 1 1 1 3 5 3 5 3 2 1 1 2 2 2
 [97] 5 2 1 2 3 2 5 2 1 1 5 3 1 2 5 3 2 5 2 1 3 1 3 3 3 1 1 2 3 3 1 2
[129] 2 1 5 5 1 1 1 2 5 3 5 1 2 2 3 5 2 3 2 4 2 3 2 4 5 2 1 3 2 5 1 4
[161] 5 2 1 1 5 2 1 1 3 2 1 2 2 3 5 1 1 2 2 1 5 2 2 2 2 3 1 2 1 1 5 1
[193] 1 5 2 2 5 2 4 2 1 1 5 1 5 2 2 5 3 2 5 5 1 2 1 2 4 1 3 2 1 5 2 1
[225] 1 5 2 2 5 2 1 2 1 1 2 3 1 1 5 2 1 1 2 2 1 3 3 1 1 4 3 1 3 2 2 5
[257] 2 1 3 2 1 2 3 1 1 1 1 3 5 2 3 2 5 1 1 2 3 1 1 1 1 1 5 1 3 2 2 2
[289] 3 5 2 5 1 1 2 3 3 5 3 4 1 5 5 1 5 2 1 1 2 2 2 3 2 1 3 1 3 2 1 2
[321] 2 4 1 5 2 2 1 2 3 5 3 1 3 2 1 1 5 3 1 1 2 1 3 2 1 5 2 2 2 1 3 1
[353] 1 1 5 2 1 1 2 1 1 5 2 5 1 2 5 4 2 4 2 1 1 2 2 1 5 1 1 1 1 1 2 3
[385] 1 5 1 1 5 3 2 4 1 1 2 5 3 1 5 2 2 1 1 2 3 5 1 2 2 1 3 1 3 1 3 1
[417] 2 1 2 2 5 5 3 1 5 1 5 5 5 1 5 1 5 1 1 1 2 2 3 2 1 2 3 1 1 1 1 5
[449] 1 2 1 5 1 3 3 2 2 1 1 2 1 3 1 5 1 1 3 2 2 1 1 5 1 5 3 5 2 3 1 1
[481] 1 3 2 1 1 3 4 2 2 5 1 1 2 5 1 2 2 2 1 1 5 4 2 2 5 2 3 2 2 1 1 5
[513] 1 2 3 2 5 3 1 1 4 1 2 3 3 1 1 2 1 1 1 1 1 2 2 3 2 1 4 2 5 2 1 3
[545] 3 2 5 5 4 1 1 2 1 3 1 2 2 5 1 5 5 1 3 3 2 5 2 2 2 1 1 3 1 1 5 2
[577] 1 5 2 2 2 2 4 3 1 1 1 2 5 3 3 1 2 1 5 2 1 2 1 3 5 3 3 1 1 3 5 2
[609] 3 2 1 5 5 2 5 1 3 5 3 2 2 2 1 5 1 1 3 3 2 2 1 3 5 1 1 1 3 2 3 5
[641] 1 3 3 1 5 1 2 3 3 1 1 2 5 5 3 2 2 1 3 2 5 5 1 3 1 1 5 5 1 3 1 5
[673] 1 1 5 5 1 1 3 3 1 2 2 2 3 1 3 3 1 3 1 5 3 2 2 2 2 5 3 1 1 1
```

The size of each cluster or number of data points in each cluster for the severity and frequency is shown below:

Severity five cluster sizes

1. **1)** 331
2. **2)** 213
3. **3)** 103
4. **4)** 19
5. **5)** 36

Frequency five cluster sizes

1. **1)** 239
2. **2)** 196
3. **3)** 124
4. **4)** 21
5. **5)** 122

The within cluster sum of squares is the sum of the squared deviations from each observation and the cluster centroid. It is a measure of the variability of the observations within each cluster and is influenced by the number of observations. In

general, a cluster that has a small sum of squares is more compact than a cluster that has a large sum of squares because as the number of observations increases, the sum of squares becomes larger. Below the within cluster sum of squares is shown by cluster for the severity and frequency:

Severity within cluster sum of squares by cluster

1) 26.18900
2) 31.75527
3) 40.39685
4) 89.28824
5) 38.85279

Frequency within cluster sum of squares by cluster

1) 157.54620
2) 43.77551
3) 75.35484
4) 34.95238
5) 28.13115

Considering that the goal of clustering is to get high similarity within each group, and low similarity between each group. Or in other words, the internal cohesion and external separation should approach 1. High similarity within a group is equal to low variance within the cluster, or within_SS and low similarity between the groups is equal to high variance between the clusters, or between_SS.

Below the BSS/TSS ratio for the severity and frequency is shown:

- Severity → between_SS / total_SS = 92.9 %
- Frequency → between_SS / total_SS = 94.6 %

For example, taking into account that k-means minimizes the within group dispersion and maximizes the between-group dispersion by assigning the samples to k (5) clusters rather than n (701) clusters, it achieves a reduction in sums of squares of 92.9 % for the severity, indicating a good fit.

The cluster means or centroids of both, the severity and frequency distributions make up the x-axis values of the fuzzy sets, while the y-axis values range from 0 to 1 (see Figure 25 and Figure 26).

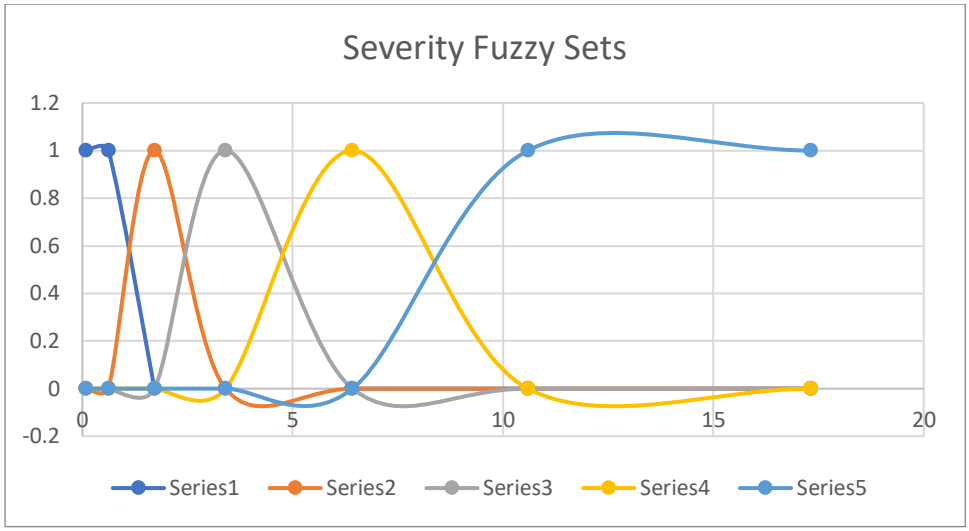


Figure 25: Severity Fuzzy Sets
Created by the author.

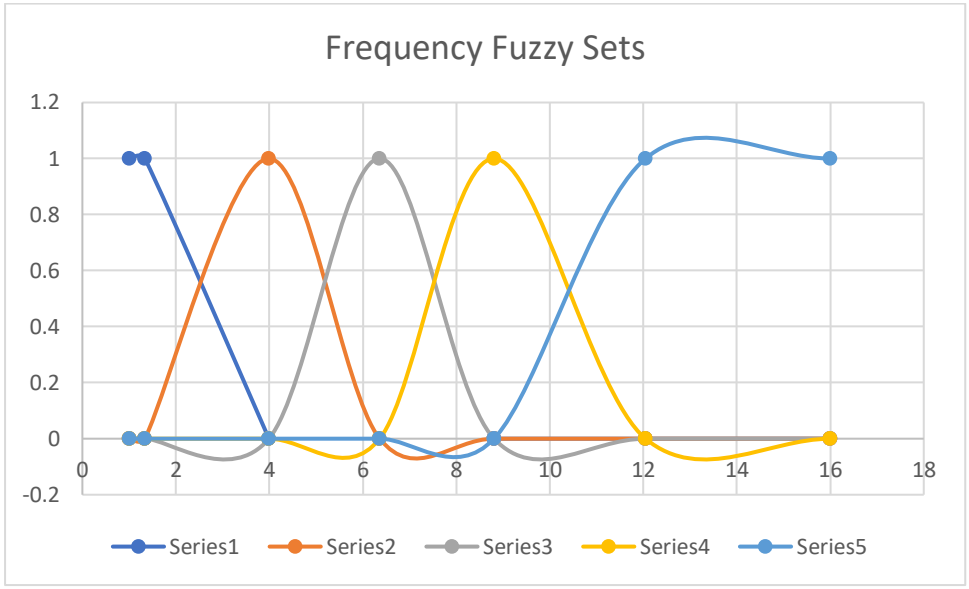


Figure 26: Frequency Fuzzy Sets
Created by the author.

Subsequently, the cumulative distribution function (CDF) of the fuzzy sets, which are the k-means of the severity and the frequency, is determined, as shown in Figure 27 and
Figure 28. The y-axis is composed of the quartiles (0, 0.25, 0.5, 0.75 and 1) and the x-axis by the five centroids of the severity or frequency distribution.

As shown in in Figure 27 and
Figure 28, a trendline following a logarithmic distribution was chosen for the severity data and the frequency data. A logarithmic trendline is a best-fit curved line that is most useful when the rate of chance in the data increases or decreases quickly and

then levels out, in this case, it increases quickly and evens out when the y-axis take the value of one (Microsoft, 2019).

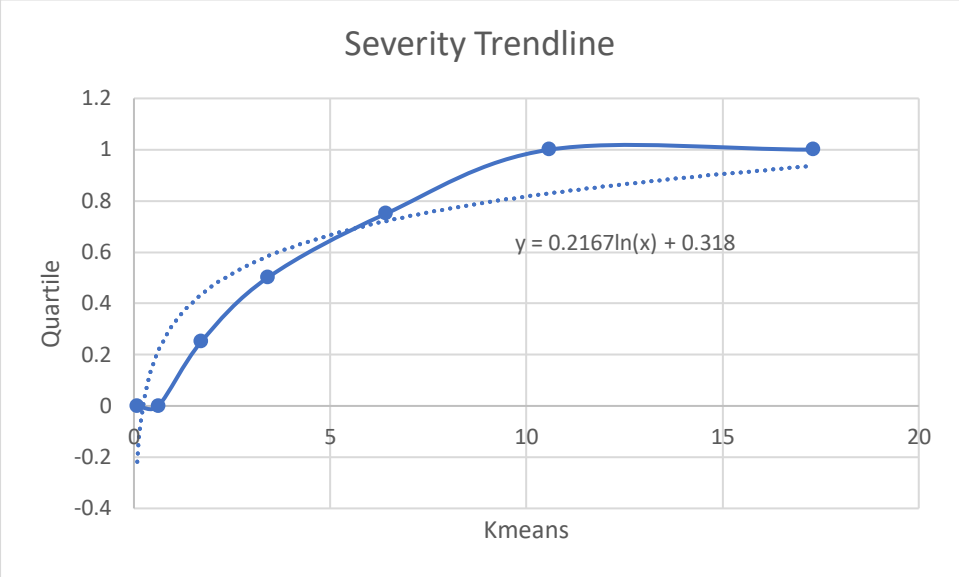


Figure 27: Severity Trendline
Created by the author.

After obtaining the severity trendline it is necessary to clear the x variable, as it is done in the process below.

$$y = 0.2167\ln(x) + 0.318$$
$$y - 0.318 = 0.2167\ln(x)$$
$$\frac{y - 0.318}{0.2167} = \ln(x)$$
$$e^{\frac{y-0.318}{0.2167}} = x$$

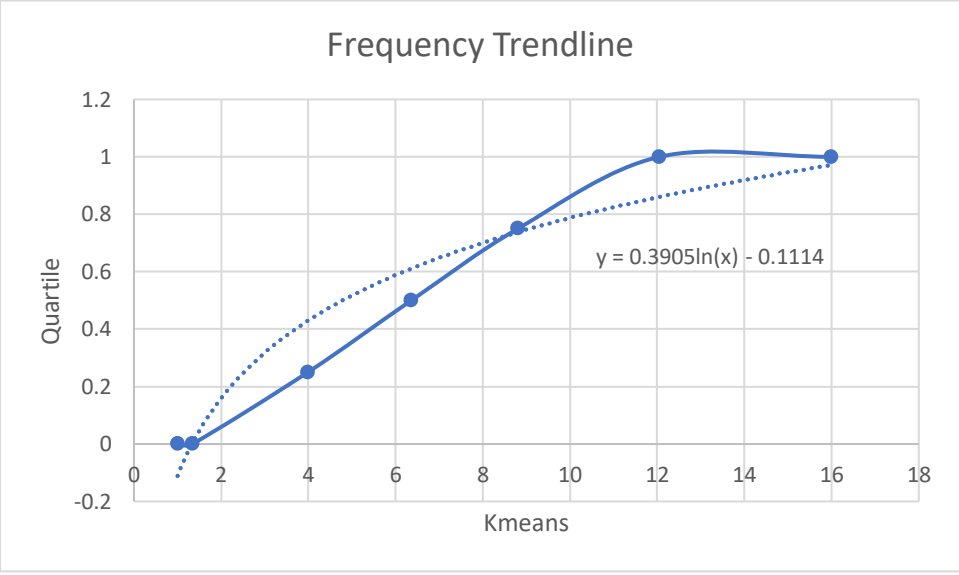


Figure 28: Frequency Trendline

Created by the author.

After obtaining the frequency trendline it is necessary to clear the x variable, as it is done in the process below.

$$y = 0.3905\ln(x) - 0.1114$$
$$y + 0.1114 = 0.3905\ln(x)$$
$$\frac{y + 0.1114}{0.3905} = \ln(x)$$
$$e^{\frac{y+0.1114}{0.3905}} = x$$

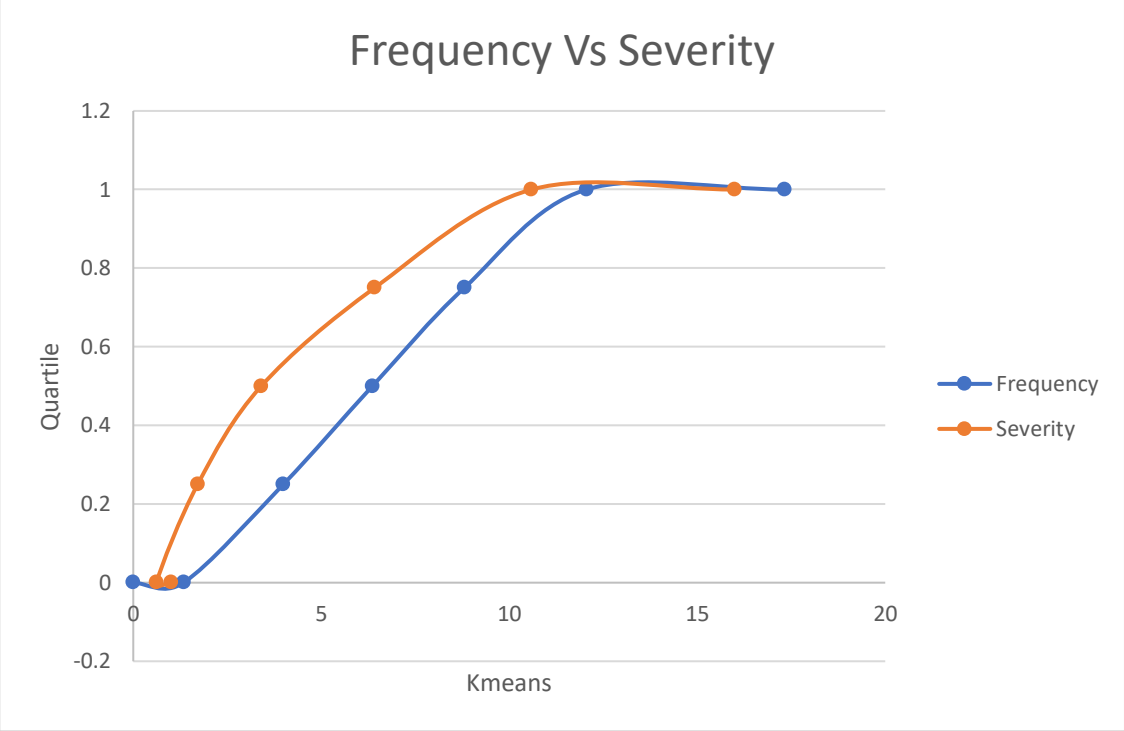


Figure 29: Frequency vs Severity
Created by the author.

The coefficient of skewness for the frequency is 0.545 and the coefficient of skewness for the severity is 2.738.This means as both values are positive, both curves are asymmetric and skewed to the right, but the severity is more, as Figure 29 shows.

After having found the k-means of the severity and frequency distributions and multiplying the number of failed transactions per day by the respective cost generated to get the LDA; equation (11) below is used to find the Euclidean distance between two points.

The Euclidean distance represents the minimum distance between a transaction failed and a frequency k-means (point 1) and a cost generated and a severity k-means (point 2). It indicates to which quadrant of the matrix does each set of data (severity, frequency) belong.

Euclidean distance = $\sqrt{(cf_k - f_n)^2 + (cs_l - s_n)^2}$ (11)

- f_n is a data point belonging to the cluster f_k
- cf_k is the mean value of the points assigned to the cluster f_k
- s_n is a data point belonging to the cluster s_l
- cs_l is the mean value of the points assigned to the cluster s_l
- *K* represents all of the five frequency cluster means
- *L* represents all of the five severity cluster means

Thus, *L* and *K* take the values from one to five considering that both distributions have five k-means. Equation (11) repeats itself 25 times for each of the 701 data points, until all possible combinations of the frequency k-means with the severity k-means where made for all data (see sheet 4:Euclidean distance of Annexe 2: Technological failures).

Then the minimum of the results of all 25 combinations will be searched in the same range (results of all 25 combinations) with the function match in excel giving a number that represents a position in the matrix.

After knowing to which quadrant of the matrix all the 701 risks belong, it is necessary to count, to know how many are in each quadrant. The result is the impact matrix (see Figure 30).

Frequency

IMPACT MATRIX				
10	6	3	2	0
55	40	17	6	6
53	38	18	9	4
119	66	37	9	7
93	63	28	10	2

Severity

Figure 30: Impact matrix
Created by the author.

If each of the values above is divided by 701, the size of the sample, then the result is the impact in $ of each risk based on its position in the matrix (see Figure 31).

Frequency

IMPACT MATRIX				
0.01426534	0.0085592	0.0042796	0.00285307	0
0.07845934	0.05706134	0.02425107	0.0085592	0.0085592
0.07560628	0.05420827	0.0256776	0.0128388	0.00570613
0.16975749	0.09415121	0.05278174	0.0128388	0.00998573
0.13266762	0.08987161	0.03994294	0.01426534	0.00285307

Severity

Figure 31: Impact matrix ($)
Created by the author.

As can be observed in Figure 30 and Figure 31 there is a much stronger color tendency (red) towards high qualitative values. This indicates a relationship between the frequency and magnitude of a risk event and the generated impact of to a certain cyber-attack activity. Risk events with higher severity tend to happen less often and risk events with lower severity happen more frequently.

3.3.2 Computational Intelligence Toolbox

The CIToolbox (v1.3_Beta)_Borroso allowed the construction and analysis of fuzzy systems taking into account the two linguistic input variables, the severity and frequency and one linguistic output variable, the aggregated loss distribution (LDA).

After pressing the connection button, in order to load the workspace of the module, the fuzzy sets for the severity and frequency where typed in.

- Frequency: [0.110954 0.331235 0.527960 0.730970 1.000000]
- Severity: [0.058423 0.161773 0.321443 0.606198 1.000000]

Both fuzzy sets where the ones obtained with the k-means clustering method using R studio and then normalized. So, the centroids obtained with the k-means clustering method are ordered from lowest to highest and each of them was divided by greater one getting the fuzzy sets shown above.

Severity cluster means:

6) 0.6186964 / 10.5898632 = 0.058423
7) 1.7131577 / 10.5898632 = 0.161773
8) 3.4040359 / 10.5898632 = 0.321443
9) 6.4195500 / 10.5898632 = 0.606198
10) 10.5898632 / 10.5898632 = 1

Frequency cluster means:

6) 1.336735 / 12.047619 = 0.110954
7) 3.990599 / 12.047619 = 0.331235
8) 6.360656 / 12.047619 = 0.527960
9) 8.806452 / 12.047619 = 0.730970
10) 12.047619 / 12.047619 = 1

Then, as shown in Figure 32 the number 5 was typed in when the system asked for the number of fuzzy sets or qualities that the output variable will have, taking into account that the final matrix will have 5 levels of risk, that are:

- 0: Very Low, 1: Low, 2: Medium, 2: High, 4: Very High

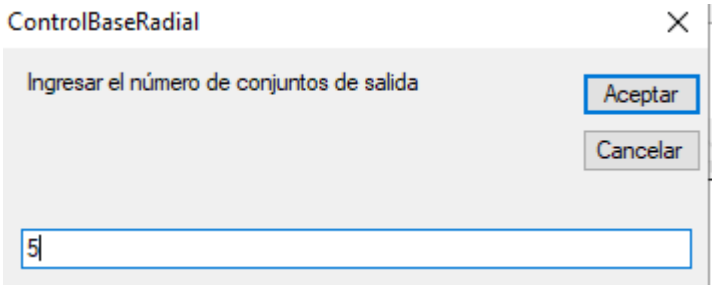
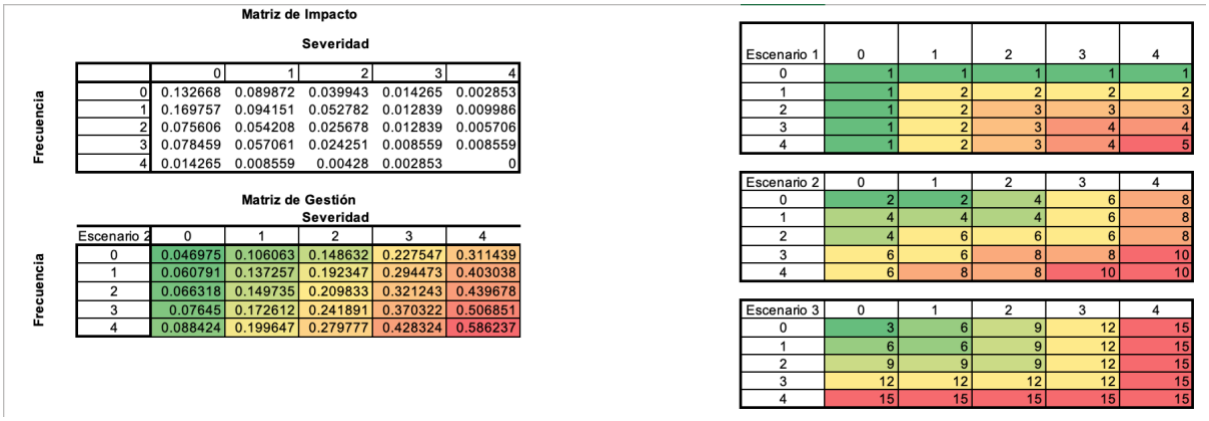


Figure 32: Number of fuzzy sets for the output
Created by the author.

Later, the impact and management matrix developed previously where copied in the decision-making excel sheet (see Figure 33).



Matriz de Impacto

Severidad

Frecuencia	0	1	2	3	4
0	0.132668	0.089872	0.039943	0.014265	0.002853
1	0.169757	0.094151	0.052782	0.012839	0.009986
2	0.075606	0.054208	0.025678	0.012839	0.005706
3	0.078459	0.057061	0.024251	0.008559	0.008559
4	0.014265	0.008559	0.00428	0.002853	0

Matriz de Gestión

Severidad

Frecuencia / Escenario 2	0	1	2	3	4
0	0.046975	0.106063	0.148632	0.227547	0.311439
1	0.060791	0.137257	0.192347	0.294473	0.403038
2	0.066318	0.149735	0.209833	0.321243	0.439678
3	0.07645	0.172612	0.241891	0.370322	0.506851
4	0.088424	0.199647	0.279777	0.428324	0.586237

Escenario 1	0	1	2	3	4
0	1	1	1	1	1
1	1	2	2	2	2
2	1	2	3	3	3
3	1	2	3	4	4
4	1	2	3	4	5

Escenario 2	0	1	2	3	4
0	2	2	4	6	8
1	4	4	4	6	8
2	4	6	6	6	8
3	6	6	8	8	10
4	6	8	8	10	10

Escenario 3	0	1	2	3	4
0	3	6	9	12	15
1	6	6	9	12	15
2	9	9	9	12	15
3	12	12	12	12	15
4	15	15	15	15	15

Figure 33: Decision-making sheet
Created by the author.

After configuring the fuzzy sets and the decision maker, the values of the linguistic input variables (severity and frequency) were copied in the estimation sheet. But first, given that the original sample contained only 701 data-points for the severity and frequency and 1000 where needed, the sample formula in R studio was used, as shown below.

- Frequency<- sample(Frequency1, size=1000, replace = TRUE)
- Severity <- sample(Severity1, size=1000, replace = TRUE)

The sample formula takes a sample of the specified size from the elements of x (frequency or severity vector), operating either with or without replacement. By default sample() randomly reorders the elements passed as the first argument. This means that the default size is the size of the passed array. Replace=TRUE makes sure that no element occurs twice.

Also, the 1000 data-points for the severity and frequency where normalized dividing each data-point by the maximum data-point. The frequency was divided by 16 and the severity by 12.4245.

The 1000 normalized data-point for the severity and frequency where the ones copied in the estimation sheet.

Finally, the number of data to asses is typed in, as shown in Figure 34.

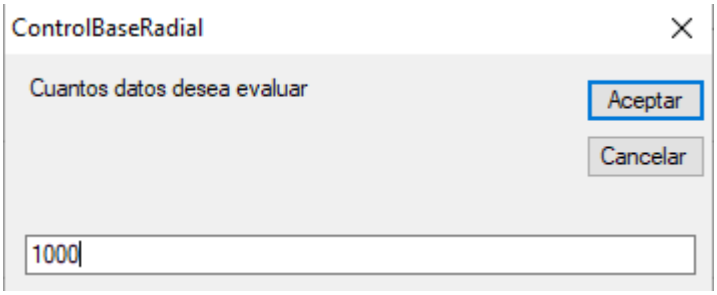


Figure 34: Number of data to asses
Created by the author.

The result of this process is the aggregated loss distribution function which shows the corporation when it does not apply any management, it is shown in the estimation sheet in Annexe 3: Fuzzy System.

The same process is repeated changing the management matrix and considering 3 scenarios (low management, medium management and high management).

The management matrix for each scenario is obtained by multiplying each value of the original management matrix by its corresponding value in each scenario matrix. For example, for scenario one 0.46975 is multiplied by 1, 0.089872 is also multiplied by 1, and so on.

The resulting 3 management matrices, one for each scenario, are shown below in Figure 35, Figure 36 and Figure 37.

		Severity				
Frequency	Escenario 1	0	1	2	3	4
	0	0.046975	0.106063	0.148632	0.227547	0.311439
	1	0.060791	0.274515	0.384693	0.588945	0.806076
	2	0.066318	0.299471	0.629498	0.963729	1.319034
	3	0.07645	0.345223	0.725672	1.481287	2.027404
	4	0.088424	0.399294	0.839331	1.713296	2.931186

Figure 35: Management matrix for scenario 1
Created by the author.

		Severity				
Frequency	Escenario 2	0	1	2	3	4
	0	0.09395	0.212125	0.594526	1.365282	2.491508
	1	0.243165	0.54903	0.769387	1.766836	3.224305
	2	0.265271	0.898412	1.258996	1.927457	3.517424
	3	0.458697	1.03567	1.935124	2.962573	5.06851
	4	0.530541	1.597177	2.238216	4.283239	5.862373

Figure 36: Management matrix for scenario 2
Created by the author.

Frequency	Severity				
Escenario 3	0	1	2	3	4
0	0.140925	0.636375	1.337684	2.730565	4.671578
1	0.364747	0.823544	1.73112	3.533672	6.045572
2	0.596859	1.347618	1.888495	3.854915	6.595169
3	0.917394	2.071339	2.902686	4.44386	7.602765
4	1.326353	2.994707	4.196655	6.424858	8.793559

Figure 37: Management matrix for scenario 3
Created by the author.

All three management matrices show a much stronger color tendency towards high qualitative values, which indicates a relationship between the magnitude of a risk event and the management towards the mitigation of cyberattack activity. The greater the magnitude, the greater the management and the probability that a cyberattack might only cause little damage.

To manage the cybersecurity risk, Table 6 proposes a series of activities to mitigate cyberattacks, which are related to the proper functioning of an electronic transaction system in a financial institution. The management matrix for scenario E2 is shown as an example, a level of 10 represents a combination of management activities, for example 2 (on-site intervention) * 5 (replace hardware) equals 10. This level of management is quantified by the number of times an activity is carried out per week. With respect to scenarios E1 (Weak Management) and E3 (Strong Management), these can be obtained by scaling the E2 matrix.

Table 6: Management activities and risk management matrix for the moderate management scenario (2)

Level	Description
1	Specific intervention
2	On-site intervention
3	General intervention
4	System maintenance
5	Replace hardware

Scenario 2	Insignificant	Minor	Moderate	Critical	Catastrophic
Rare	2	2	4	6	8
Unlikely	4	4	4	6	8
Possible	4	6	6	6	8
Likely	6	6	8	8	10
Almost Certain	6	8	8	10	10

Created by the author.

3.4 Validate the model taking into account the behavior of the aggregated distribution of losses and the coverage percentage with regard to the expected losses

To validate the model, it was necessary to determine the distribution of each set of data, the original frequency, the original severity, the original LDA, the LDA_1, the LDA_2, the LDA_3 and the LDA_4 shown in Annexe 3: Fuzzy System.

Figure 38 shows how ALLFITDIST for the original LDA data plots the Probability Density Function (PDF) of the lognormal distribution, the generalized pareto

distribution, the birnbaumsaunders distribution and the loglogistic distribution in that order of fit. The Negative of the log likelihood (NLogL), the Akaike information criterion (AIC), the corrected Akaike's Information Criterion (AICc) and the Bayesian Information Criterion (BIC) ordered by the best fitted distributions from the smallest value to largest (see Figure 39).

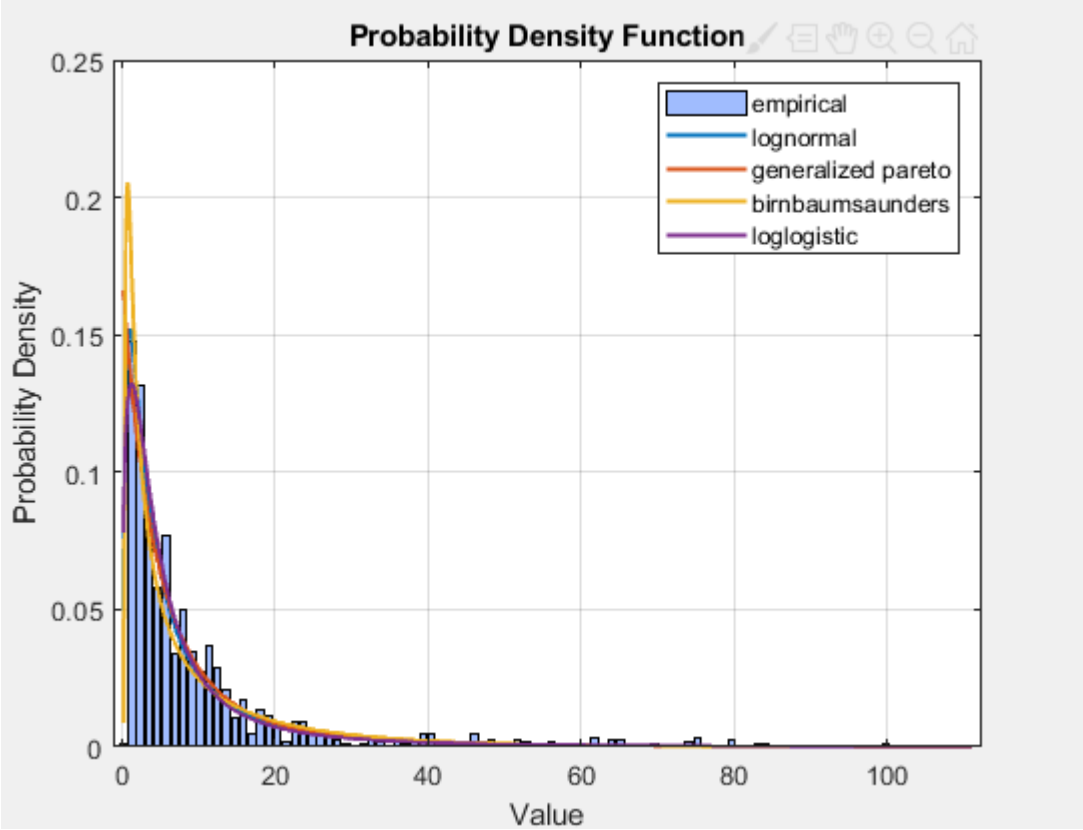


Figure 38: Distributions that best fit the original LDA data
Created by the author.

Fields	DistName	NLogL	BIC	AIC	AICc
1	'lognormal'	3.1755e+03	6.3648e+03	6.3550e+03	6.3550e+03
2	'generalized ...	3.1726e+03	6.3659e+03	6.3512e+03	6.3512e+03
3	'birnbaumsa...	3.1838e+03	6.3815e+03	6.3716e+03	6.3717e+03
4	'loglogistic'	3.1919e+03	6.3975e+03	6.3877e+03	6.3877e+03
5	'generalized ...	3.2086e+03	6.4380e+03	6.4233e+03	6.4233e+03
6	'inverse gaus...	3.2149e+03	6.4436e+03	6.4338e+03	6.4338e+03
7	'weibull'	3.2267e+03	6.4673e+03	6.4574e+03	6.4575e+03
8	'gamma'	3.2439e+03	6.5016e+03	6.4918e+03	6.4918e+03
9	'exponential'	3.2603e+03	6.5275e+03	6.5226e+03	6.5226e+03
10	'nakagami'	3.3628e+03	6.7395e+03	6.7296e+03	6.7297e+03
11	'tlocationsca...	3.5443e+03	7.1093e+03	7.0946e+03	7.0946e+03
12	'logistic'	3.8105e+03	7.6348e+03	7.6250e+03	7.6250e+03
13	'normal'	4.0444e+03	8.1027e+03	8.0929e+03	8.0929e+03
14	'rayleigh'	4.4255e+03	8.8578e+03	8.8529e+03	8.8529e+03
15	'rician'	4.4255e+03	8.8647e+03	8.8549e+03	8.8549e+03
16	'extreme val...	4.5286e+03	9.0710e+03	9.0612e+03	9.0612e+03

Figure 39: Valid distributions for the original LDA data sorted by NLogL, BIC, AIC and AICc
Created by the author.

Figure 40 shows how ALLFITDIST for the original frequency data plots the Probability Density Function (PDF) of the negative binomial distribution, the poisson distribution and the binomial distribution in that order of fit. The Negative of the log likelihood (NLogL), the Akaike information criterion (AIC), the corrected Akaike's Information Criterion (AICc) and the Bayesian Information Criterion (BIC) ordered by the best fitted distributions from the smallest value to largest (see Figure 41).

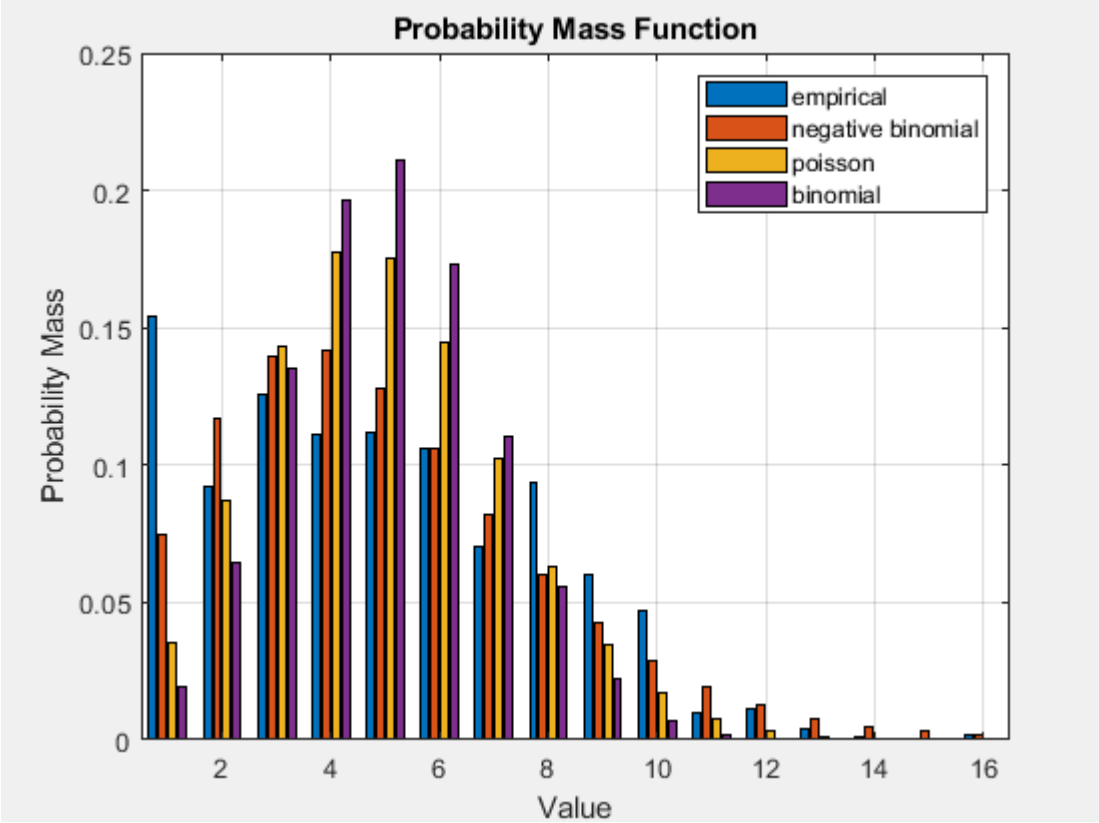


Figure 40: Distributions that best fit the original frequency data
Created by the author.

1x3 struct with 11 fields

Fields	DistName	NLogL	BIC	AIC	AICc
1	'negative bin...	2.4502e+03	4.9141e+03	4.9043e+03	4.9043e+03
2	'poisson'	2.5554e+03	5.1176e+03	5.1127e+03	5.1127e+03
3	'binomial'	2.7832e+03	5.5802e+03	5.5704e+03	5.5704e+03

Figure 41: Valid distributions for the original frequency data sorted by NLogL, BIC, AIC and AICc
Created by the author.

Figure 42 shows how ALLFITDIST for the original severity data plots the Probability Density Function (PDF) of the birnbaumsaunders distribution, the lognormal distribution, the inverse gaussian distribution and the loglogistic distribution in that order of fit. The Negative of the log likelihood (NLogL), the Akaike information criterion (AIC), the corrected Akaike's Information Criterion (AICc) and the Bayesian Information Criterion (BIC) ordered by the best fitted distributions from the smallest value to largest (see Figure 43).

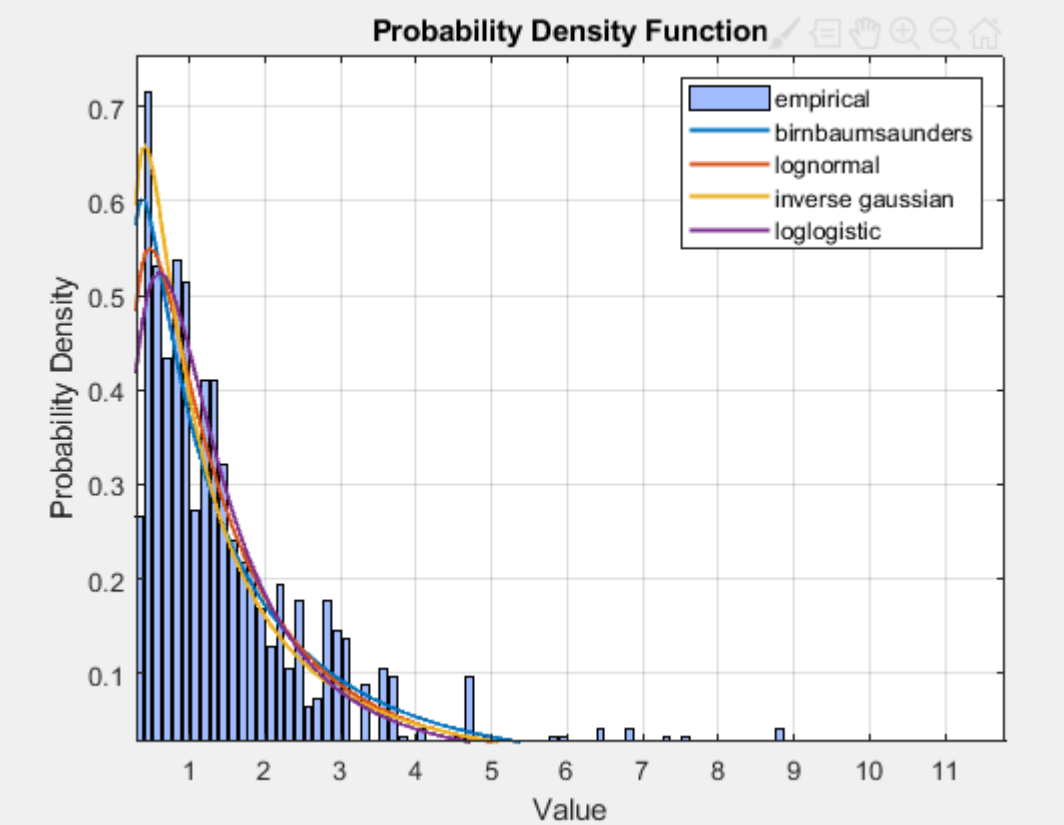


Figure 42: Distributions that best fit the original severity data
Created by the author.

1x16 struct with 11 fields

Fields	DistName	NLogL	BIC	AIC	AICc
1	'birnbaumsa...	1.5551e+03	3.1239e+03	3.1141e+03	3.1141e+03
2	'lognormal'	1.5559e+03	3.1256e+03	3.1158e+03	3.1158e+03
3	'inverse gaus...	1.5601e+03	3.1340e+03	3.1242e+03	3.1242e+03
4	'loglogistic'	1.5708e+03	3.1555e+03	3.1457e+03	3.1457e+03
5	'generalized ...	1.5722e+03	3.1652e+03	3.1504e+03	3.1505e+03
6	'generalized ...	1.5770e+03	3.1746e+03	3.1599e+03	3.1599e+03
7	'gamma'	1.6135e+03	3.2408e+03	3.2310e+03	3.2310e+03
8	'weibull'	1.6241e+03	3.2620e+03	3.2522e+03	3.2522e+03
9	'exponential'	1.6289e+03	3.2646e+03	3.2597e+03	3.2597e+03
10	'nakagami'	1.7124e+03	3.4386e+03	3.4288e+03	3.4288e+03
11	'tlocationsca...	1.8296e+03	3.6799e+03	3.6652e+03	3.6652e+03
12	'logistic'	1.9775e+03	3.9688e+03	3.9590e+03	3.9590e+03
13	'normal'	2.1102e+03	4.2343e+03	4.2245e+03	4.2245e+03
14	'rayleigh'	2.1408e+03	4.2884e+03	4.2835e+03	4.2835e+03
15	'rician'	2.1408e+03	4.2953e+03	4.2855e+03	4.2855e+03
16	'extreme val...	2.4774e+03	4.9685e+03	4.9587e+03	4.9587e+03

Figure 43: Valid distributions for the original severity data sorted by NLogL, BIC, AIC and AICc
Created by the author.

Figure 44 shows how ALLFITDIST for the LDA_1 (no management) data plots the Probability Density Function (PDF) of the generalized pareto distribution, the weibull distribution, the nakagami distribution and the beta distribution in that order of fit. The Negative of the log likelihood (NLogL), the Akaike information criterion (AIC), the corrected Akaike's Information Criterion (AICc) and the Bayesian Information Criterion (BIC) ordered by the best fitted distributions from the smallest value to largest (see Figure 45).

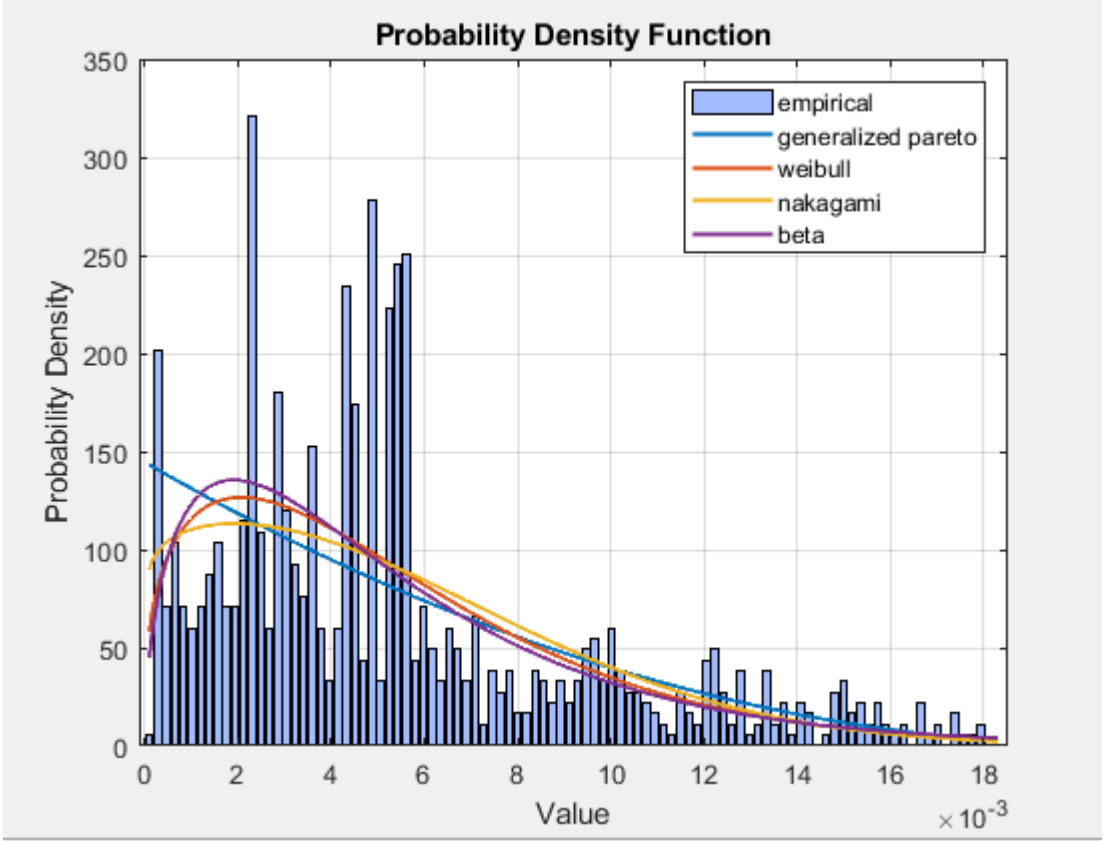


Figure 44: Distributions that best fit the LDA_1 data – no management
Created by the author.

1x17 struct with 11 fields

Fields	DistName	NLogL	BIC	AIC	AICc
1	'generalized ...	-4.2988e+03	-8.5768e+03	-8.5916e+03	-8.5915e+03
2	'weibull'	-4.2941e+03	-8.5744e+03	-8.5842e+03	-8.5842e+03
3	'nakagami'	-4.2909e+03	-8.5680e+03	-8.5778e+03	-8.5778e+03
4	'beta'	-4.2872e+03	-8.5605e+03	-8.5704e+03	-8.5703e+03
5	'gamma'	-4.2868e+03	-8.5598e+03	-8.5696e+03	-8.5696e+03
6	'generalized ...	-4.2623e+03	-8.5038e+03	-8.5186e+03	-8.5185e+03
7	'exponential'	-4.2340e+03	-8.4610e+03	-8.4659e+03	-8.4659e+03
8	'loglogistic'	-4.2234e+03	-8.4331e+03	-8.4429e+03	-8.4429e+03
9	'lognormal'	-4.1811e+03	-8.3484e+03	-8.3582e+03	-8.3582e+03
10	'rayleigh'	-4.1338e+03	-8.2607e+03	-8.2656e+03	-8.2656e+03
11	'rician'	-4.1338e+03	-8.2538e+03	-8.2636e+03	-8.2636e+03
12	'tlocationsca...	-4.1351e+03	-8.2495e+03	-8.2642e+03	-8.2642e+03
13	'logistic'	-4.1308e+03	-8.2479e+03	-8.2577e+03	-8.2577e+03
14	'normal'	-4.1114e+03	-8.2089e+03	-8.2187e+03	-8.2187e+03
15	'birnbaumsa...	-4.1058e+03	-8.1978e+03	-8.2076e+03	-8.2076e+03
16	'inverse gaus...	-4.0178e+03	-8.0219e+03	-8.0317e+03	-8.0317e+03
17	'extreme val...	-3.8968e+03	-7.7798e+03	-7.7897e+03	-7.7896e+03

Figure 45: Valid distributions for the LDA_1 data sorted by NLogL, BIC, AIC and AICc – no management
Created by the author.

Figure 46 shows how ALLFITDIST for the LDA_2 (scenario 1: weak management) data plots the Probability Density Function (PDF) of the generalized pareto distribution, the weibull distribution, the beta distribution and the exponential distribution in that order of fit. The Negative of the log likelihood (NLogL), the Akaike information criterion (AIC), the corrected Akaike's Information Criterion (AICc) and the Bayesian Information Criterion (BIC) ordered by the best fitted distributions from the smallest value to largest (see Figure 47).

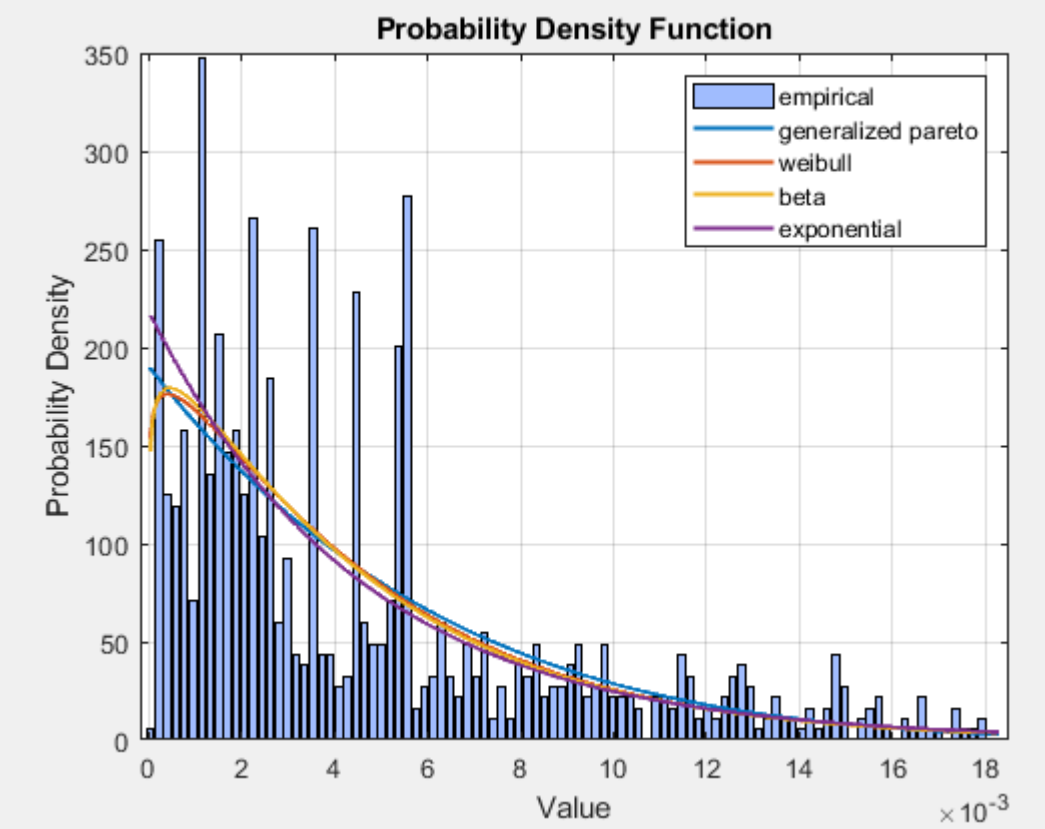


Figure 46: Distributions that best fit the LDA_2 data - weak management
Created by the author.

Fields	DistName	NLogL	BIC	AIC	AICc
1	'generalized ...	-4.3977e+03	-8.7746e+03	-8.7893e+03	-8.7893e+03
2	'weibull'	-4.3881e+03	-8.7623e+03	-8.7721e+03	-8.7721e+03
3	'beta'	-4.3875e+03	-8.7611e+03	-8.7710e+03	-8.7710e+03
4	'exponential'	-4.3839e+03	-8.7609e+03	-8.7658e+03	-8.7658e+03
5	'gamma'	-4.3872e+03	-8.7607e+03	-8.7705e+03	-8.7705e+03
6	'nakagami'	-4.3796e+03	-8.7453e+03	-8.7551e+03	-8.7551e+03
7	'loglogistic'	-4.3195e+03	-8.6252e+03	-8.6350e+03	-8.6350e+03
8	'generalized ...	-4.3198e+03	-8.6189e+03	-8.6336e+03	-8.6336e+03
9	'lognormal'	-4.3022e+03	-8.5906e+03	-8.6004e+03	-8.6004e+03
10	'birnbaumsa...	-4.2279e+03	-8.4420e+03	-8.4518e+03	-8.4518e+03
11	'tlocationsca...	-4.1004e+03	-8.1801e+03	-8.1948e+03	-8.1948e+03
12	'inverse gaus...	-4.0953e+03	-8.1768e+03	-8.1866e+03	-8.1866e+03
13	'logistic'	-4.0930e+03	-8.1721e+03	-8.1820e+03	-8.1819e+03
14	'normal'	-4.0709e+03	-8.1280e+03	-8.1378e+03	-8.1378e+03
15	'rayleigh'	-3.9704e+03	-7.9338e+03	-7.9388e+03	-7.9388e+03
16	'rician'	-3.9704e+03	-7.9269e+03	-7.9368e+03	-7.9367e+03
17	'extreme val...	-3.8446e+03	-7.6754e+03	-7.6852e+03	-7.6852e+03

Figure 47: Valid distributions for the LDA_2 data sorted by NLogL, BIC, AIC and AICc - weak management
Created by the author.

Figure 48 shows how ALLFITDIST for the LDA_3 (scenario 2: medium management) data plots the Probability Density Function (PDF) of the generalized pareto distribution, the exponential distribution, the weibull distribution and the beta distribution in that order of fit. The Negative of the log likelihood (NLogL), the Akaike information criterion (AIC), the corrected Akaike's Information Criterion (AICc) and the Bayesian Information Criterion (BIC) ordered by the best fitted distributions from the smallest value to largest (see Figure 49).

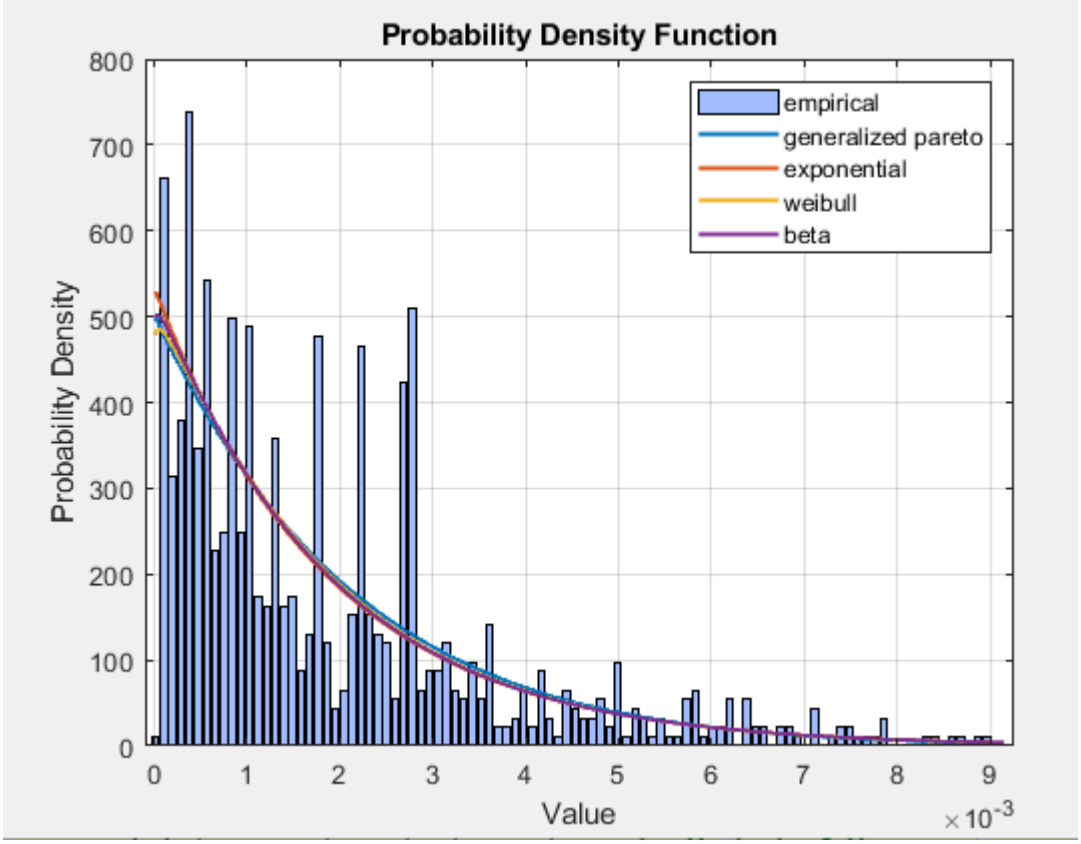


Figure 48: Distributions that best fit the LDA_3 data - medium management
Created by the author.

Fields	DistName	NLogL	BIC	AIC	AICc
1	'generalized ...	-5.2874e+03	-1.0554e+04	-1.0569e+04	-1.0569e+04
2	'exponential'	-5.2793e+03	-1.0552e+04	-1.0557e+04	-1.0557e+04
3	'weibull'	-5.2797e+03	-1.0546e+04	-1.0555e+04	-1.0555e+04
4	'beta'	-5.2795e+03	-1.0545e+04	-1.0555e+04	-1.0555e+04
5	'gamma'	-5.2794e+03	-1.0545e+04	-1.0555e+04	-1.0555e+04
6	'nakagami'	-5.2710e+03	-1.0528e+04	-1.0538e+04	-1.0538e+04
7	'loglogistic'	-5.2010e+03	-1.0388e+04	-1.0398e+04	-1.0398e+04
8	'generalized ...	-5.1972e+03	-1.0374e+04	-1.0388e+04	-1.0388e+04
9	'lognormal'	-5.1815e+03	-1.0349e+04	-1.0359e+04	-1.0359e+04
10	'birnbaumsa...	-5.1042e+03	-1.0195e+04	-1.0204e+04	-1.0204e+04
11	'tlocationsca...	-4.9847e+03	-9.9486e+03	-9.9634e+03	-9.9633e+03
12	'logistic'	-4.9686e+03	-9.9233e+03	-9.9331e+03	-9.9331e+03
13	'inverse gaus...	-4.9355e+03	-9.8572e+03	-9.8670e+03	-9.8670e+03
14	'normal'	-4.9234e+03	-9.8330e+03	-9.8428e+03	-9.8428e+03
15	'rayleigh'	-4.7744e+03	-9.5419e+03	-9.5468e+03	-9.5468e+03
16	'rician'	-4.7744e+03	-9.5350e+03	-9.5448e+03	-9.5448e+03
17	'extreme val...	-4.6501e+03	-9.2864e+03	-9.2962e+03	-9.2962e+03

Figure 49: Valid distributions for the LDA_3 data sorted by NLogL, BIC, AIC and AICc - medium management
Created by the author.

Figure 50 shows how ALLFITDIST for the LDA_4 (scenario 3: strong management) data plots the Probability Density Function (PDF) of the generalized pareto distribution, the exponential distribution, the weibull distribution and the gamma distribution in that order of fit. The Negative of the log likelihood (NLogL), the Akaike information criterion (AIC), the corrected Akaike's Information Criterion (AICc) and the Bayesian Information Criterion (BIC) ordered by the best fitted distributions from the smallest value to largest (see Figure 51).

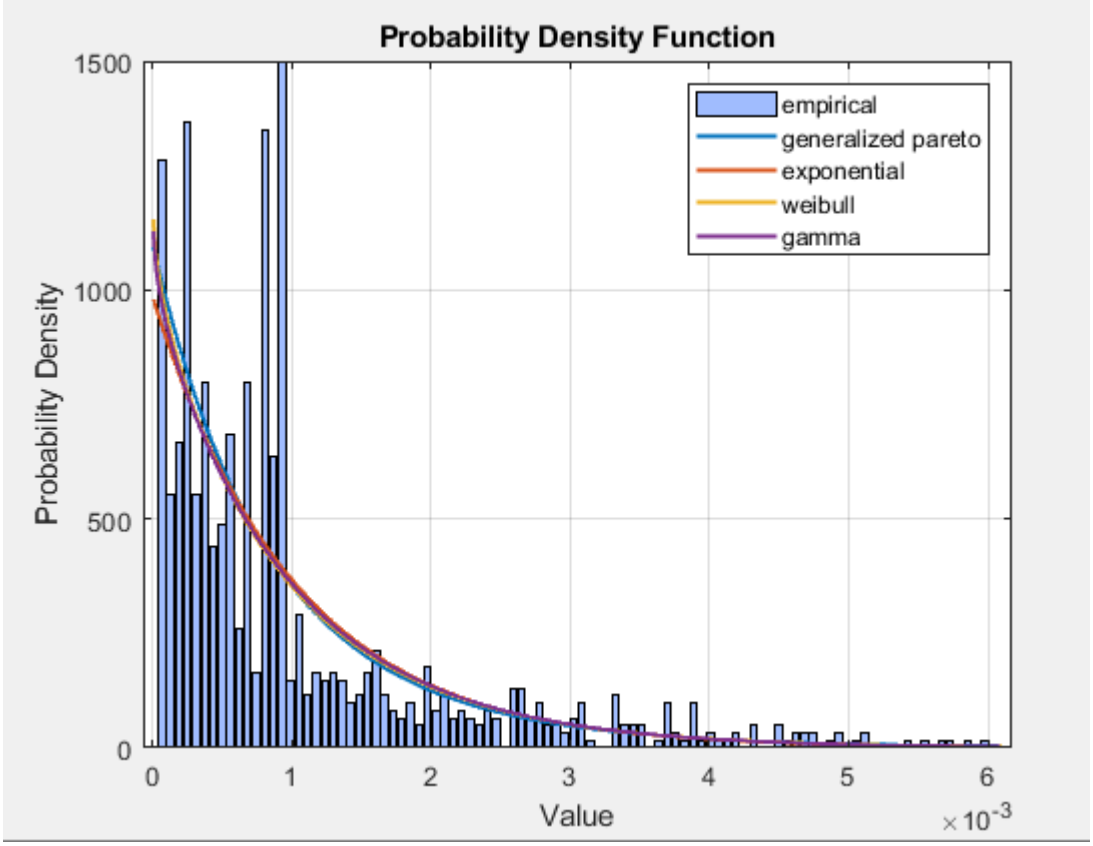


Figure 50: Distributions that best fit the LDA_4 data - strong management
Created by the author.

Fields	DistName	NLogL	BIC	AIC	AICc
1	'generalized ...	-5.9050e+03	-1.1789e+04	-1.1804e+04	-1.1804e+04
2	'exponential'	-5.8941e+03	-1.1781e+04	-1.1786e+04	-1.1786e+04
3	'weibull'	-5.8954e+03	-1.1777e+04	-1.1787e+04	-1.1787e+04
4	'gamma'	-5.8947e+03	-1.1776e+04	-1.1785e+04	-1.1785e+04
5	'beta'	-5.8947e+03	-1.1776e+04	-1.1785e+04	-1.1785e+04
6	'loglogistic'	-5.8545e+03	-1.1695e+04	-1.1705e+04	-1.1705e+04
7	'nakagami'	-5.8492e+03	-1.1685e+04	-1.1694e+04	-1.1694e+04
8	'generalized ...	-5.8469e+03	-1.1673e+04	-1.1688e+04	-1.1688e+04
9	'lognormal'	-5.8313e+03	-1.1649e+04	-1.1659e+04	-1.1659e+04
10	'birnbaumsa...	-5.7470e+03	-1.1480e+04	-1.1490e+04	-1.1490e+04
11	'tlocationsca...	-5.6255e+03	-1.1230e+04	-1.1245e+04	-1.1245e+04
12	'inverse gaus...	-5.5969e+03	-1.1180e+04	-1.1190e+04	-1.1190e+04
13	'logistic'	-5.5045e+03	-1.0995e+04	-1.1005e+04	-1.1005e+04
14	'normal'	-5.4050e+03	-1.0796e+04	-1.0806e+04	-1.0806e+04
15	'rayleigh'	-5.2158e+03	-1.0425e+04	-1.0430e+04	-1.0430e+04
16	'rician'	-5.2158e+03	-1.0418e+04	-1.0428e+04	-1.0428e+04
17	'extreme val...	-5.0739e+03	-1.0134e+04	-1.0144e+04	-1.0144e+04

Figure 51: Valid distributions for the LDA_4 data sorted by NLogL, BIC, AIC and AICc - strong management
Created by the author.

Taking into account that the LDA distributions are heavily tailed distributions, such as Weibull, Lognormal, Loglogistic or Generalized Pareto; the LDA distributions obtained were modeled using the distribution fitter app of MATLAB according to the Loglogistic and Weibull distributions respectively.

Figure 52 and Figure 53 show the structure and the form taken by the LDAs for each of the management scenarios defined above, as well as for the reference LDA.

- LDA_1: reference LDA or original LDA, has no management at all.
- LDA_2: LDA found with scenario 1, with weak management.
- LDA_3: LDA found with scenario 2, with normal management.
- LDA_4: LDA found with scenario 3, with strong management.

The structural stability of the model can be evidenced through the evolution of the LDAs towards increasingly slender distributions (not as heavy tailed, lighter) that converge to zero faster. Also, through the evolution of the asymmetry or skewness coefficient towards increasingly higher positive values, for equally stronger managements. Consequently, the probability of catastrophic events happening decreases.

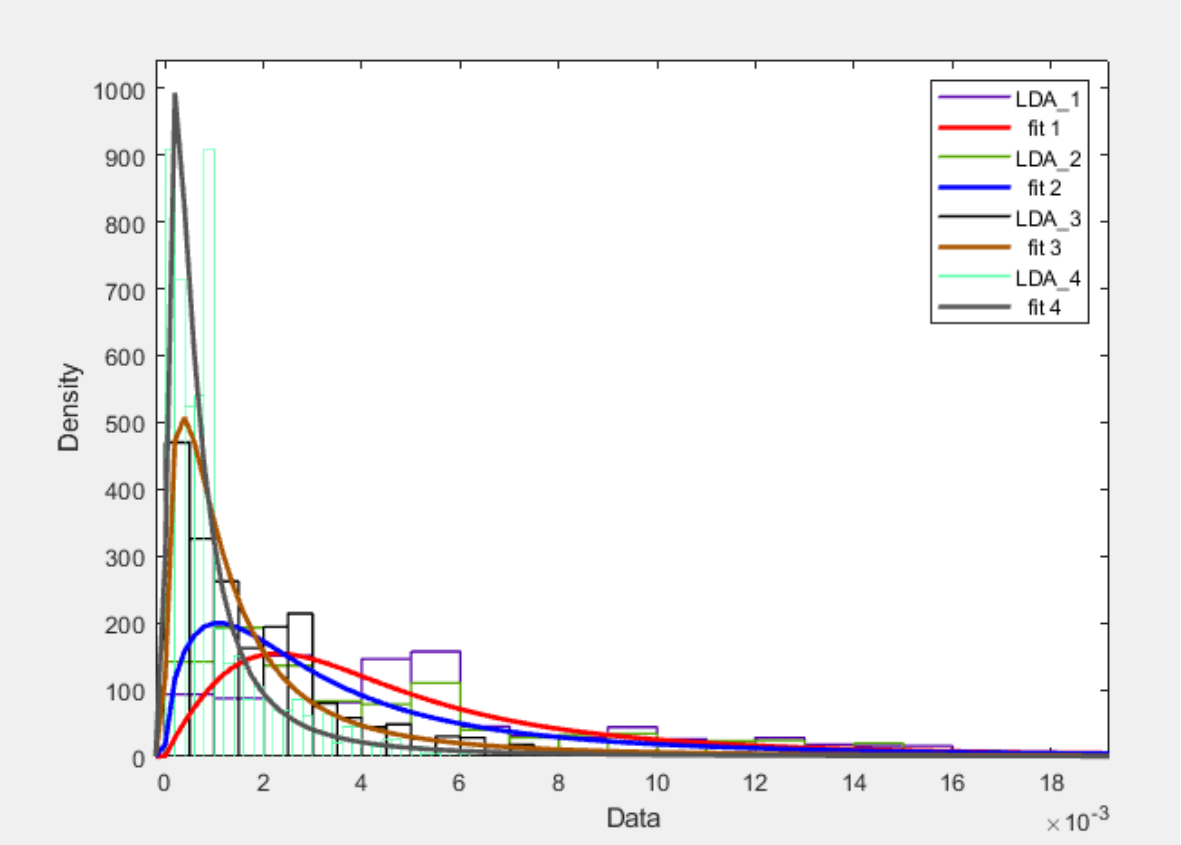


Figure 52: Fit LDA curves as Log-logistic
Created by the author.

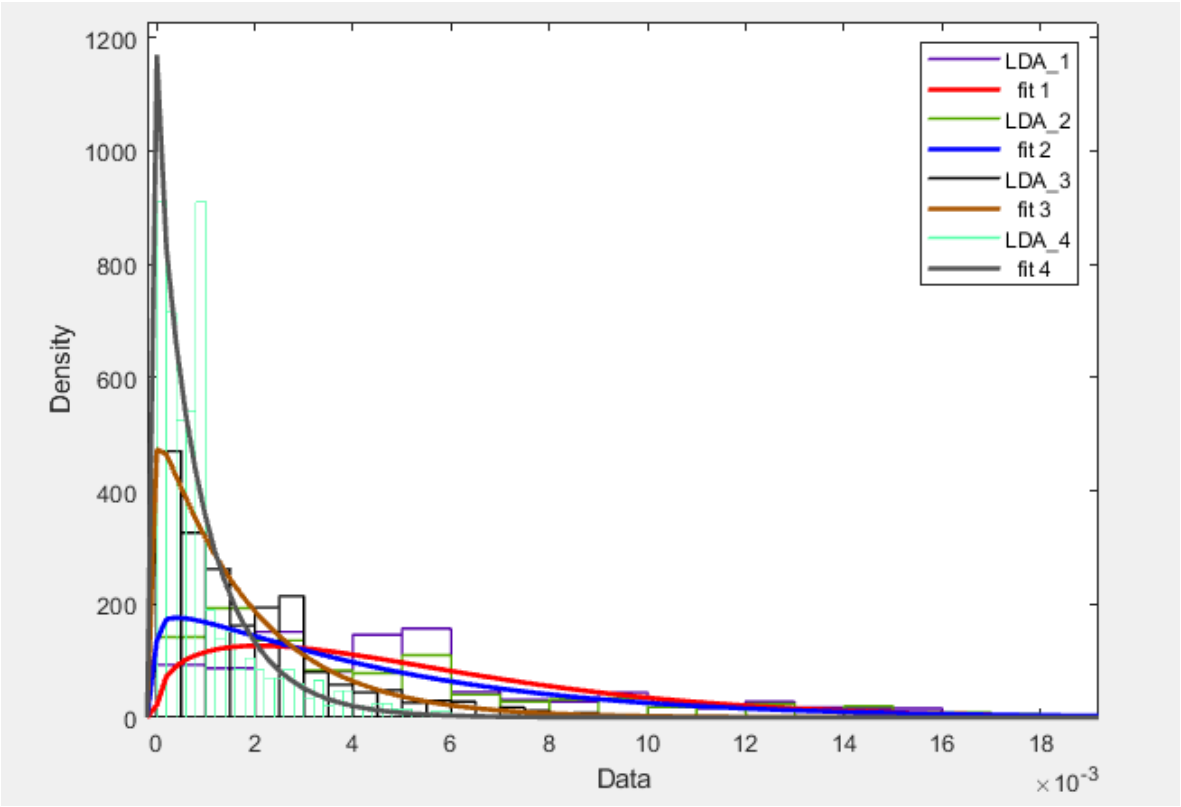


Figure 53: Fit LDA curves as Weibull
Created by the author.

In Table 7, Figure 52 and Figure 53 the dimensional stability that has been reached by applying the model can be observed by means of the evolution of the LDA distributions. The LDA distributions take an increasingly slender shape (not as heavy tailed), due to better management, which can also be evidenced by the asymmetry or skewness coefficient that tends towards increasingly higher positive values. Also through the decrease experienced by the OpVar, as well as the decrease experienced by the coverage rate of the EL and increase of the coverage rate of the UL. As the expected losses (EL) and the unexpected losses (UL) decrease as the LDA distribution evolves according to the scenarios, we can observe the impact of management carried out by the decision makers in an organization with respect to the coverage of the risk of cyberattacks. Consequently, we can obtain a more objective valuation of an insurance policy that covers cyberattacks.

Table 7: Description of the LDA distributions for each of the proposed scenarios.

Calculations	LDA	LDA1	LDA2	LDA3	LDA4
EL *(Mean)*	9.5859	0.0053	0.0046	0.0019	0.001
OpVar *(percentile 99.9%)*	105.238	0.0181	0.0181	0.0091	0.006
UL *(OpVar - EL)*	95.6521	0.0128	0.0135	0.0072	0.005
Asymmetry coefficient *(skewness)*	3.2046	1.1084	1.2329	1.4741	1.9691
EL/OpVar	0.0911	0.2928	0.2541	0.2088	0.1667
UL/OpVar	0.9089	0.7072	0.7459	0.7912	0.8333

Created by the author.

4 CONCLUSIONS AND FINAL CONSIDERATIONS

The structure of the proposed model allowed the OpVar estimation for cyber-risk faced by a financial institution. Thus, integrating in a single model the representation of the frequency and the severity as linguistic random variables. Furthermore, the construction of the management and impact matrices considering the experts judgment based on the structure of a fuzzy AHP model. An adaptation and learning process was implemented that allows the configuration of the fuzzy neural structure of the model, in accordance with the aggregated loss distribution (LDA) defined by the Basel II accord set by The Basel Committee on Banking Supervision (BCBS).

The LDA distributions obtained as a result of applying different management scenarios evidenced the structural stability of the model. Stability in terms of the structure taken by the LDA distributions, as well as the dimensional stability, proven by the evolution of the asymmetry or skewness coefficient towards positive values with greater magnitudes, which in turn caused lower OpVar values due to better management.

It is important to highlight that the proposed model achieved much lower OpVar values for each of the proposed scenarios (no management, weak management, medium management and strong management), than the OpVar obtained with the original LDA using the referenced methodology established by the Basel Committee on Banking Supervision (BCBS) for this type of risk. However, the magnitude of the impact of the risk events grouped by an aggregated loss distribution (LDA) for each scenario always remained above the impact of the risk events grouped by the referenced LDA, which demonstrates the importance of the tail of the distributions with regard to the mitigation of cyberrisk.

In general, risk analysis can be carried out from the perspective of financial organizations, as well as from the perspective of an insurer. That is why this model becomes a fundamental tool for the estimation of operational risk derived from cybersecurity operations not yet materialized. Also, it can be constituted as a base model for the development of parametric insurances, which can be configured concerning the coverage of the risk according to the expected losses (EL), the unexpected losses (UL) and the catastrophic losses (SL).

5 REFERENCES

Abul-Haggag, O. Y., & Barakat, W. (2013). Application of Fuzzy Logic for Risk Assessment using Risk Matrix. *International Journal of Emerging Technology and Advanced Engineering*, *3*(1). Retrieved from https://pdfs.semanticscholar.org/5ab7/1acbb1a88f7217762e8b0d824ccf89bbc7dd.pdf

Accenture. (2016a). *Building Confidence Solving Banking's Cybersecurity Conundrum | Accenture*. Retrieved from https://www.accenture.com/t20180228T105508Z__w__/us-en/_acnmedia/PDF-44/Accenture-Building-Confidence-Solving-Banking-Cybersecurity-Conundrum.pdf#zoom=50

Accenture. (2016b). *The Convergence of Operational Risk and Cyber Security*. Retrieved from https://www.accenture.com/t20170803T055319Z__w__/us-en/_acnmedia/PDF-7/Accenture-Cyber-Risk-Convergence-Of-Operational-Risk-And-Cyber-Security.pdf

ACME Business Consulting. Inc. (2017). *Example Cybersecurity Risk Management Program (RMP)*. Retrieved from http://examples.complianceforge.com/example-cyber-security-risk-management-framework-template-rmf.pdf

Ahmed, M. A. O. (2018). Trained Neural Networks Ensembles Weight Connections Analysis (pp. 242–251). https://doi.org/10.1007/978-3-319-74690-6_24

Al-Augby, S., Majewski, S., Majewska, A., & Nermend, K. (2014). A Comparison Of K-Means And Fuzzy C-Means Clustering Methods For A Sample Of Gulf Cooperation Council Stock Markets. *Folia Oeconomica Stetinensia*, *14*(2), 19–36. https://doi.org/10.1515/foli-2015-0001

Aliev, R. A. (Rafik A. ogly). (2013). *Fundamentals of the fuzzy logic-based generalized theory of decisions*. Springer.

Aminbakhsh, S., Gunduz, M., & Sonmez, R. (2013). Safety risk assessment using analytic hierarchy process (AHP) during planning and budgeting of construction projects. *Journal of Safety Research*, *46*, 99–105. https://doi.org/10.1016/j.jsr.2013.05.003

Anand, G., & Sameera, G. (2012). Importance of Risk Analysis and Management – The Case of Australian Real Estate Market. In *Risk Management - Current Issues and Challenges*. InTech. https://doi.org/10.5772/50669

Anthony TonyCox, L. (2008). What's Wrong with Risk Matrices? *Risk Analysis*, *28*(2), 497–512. https://doi.org/10.1111/j.1539-6924.2008.01030.x

Awad, M., & Khanna, R. (2015). Machine Learning. In *Efficient Learning Machines* (pp. 1–18). Berkeley, CA: Apress. https://doi.org/10.1007/978-1-4302-5990-9_1

Badri, M. A. (2001). A combined AHP–GP model for quality control systems.

International Journal of Production Economics, *72*(1), 27–40. https://doi.org/10.1016/S0925-5273(00)00077-3

Bank for International Settlements. (1998). Operational Risk Management Basle Committee on Banking Supervision Basle. Retrieved from http://www.bis.org/publ/bcbs42.pdf

Basel. (2003). Sound Practices for the Management and Supervision of Operational Risk. *Phytochemistry*, *62*(February), 245. https://doi.org/10.1016/S0031-9422(02)00552-6

Basel Committee on Banking Supervision. (2006). International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version, June 2006. Retrieved from http://www.bis.org/publ/bcbs128.pdf

Basel Committee on Banking Supervision. (2009). *Basel Committee on Banking Supervision Observed range of practice in key elements of Advanced Measurement Approaches (AMA)*. Retrieved from https://www.bis.org/publ/bcbs160b.pdf

Bekefi, T., Epstein, M. J., & Yuthas, K. (2011). Managing Opportunities and Risks N OT I C E TO R E A D E R S. Retrieved from http://www.cimaglobal.com/Documents/ImportedDocuments/cid_mag_managing_opportunities_and_risk_march08.pdf.pdf

Crisanto, J. C., & Prenio, J. (2017). FSI Insights Regulatory approaches to enhance banks ', (2).

Cruz, M. G., Peters, G. W., & Shevchenko, P. V. (2015). *Fundamental Aspects of Operational Risk and Insurance Analytics*. Hoboken, NJ: John Wiley & Sons, Inc. https://doi.org/10.1002/9781118573013

Danesh, D., Ryan, M. J., & Abbasi, A. (2017). A Systematic Comparison of Multi-criteria Decision Making Methods for the Improvement of Project Portfolio Management in Complex Organisations. *International Journal of Management and Decision Making*, *16*(1), 1. https://doi.org/10.1504/IJMDM.2017.10005690

del Brío, B. M., & Sanz Molina, A. (2005). Redes Neuronales y Sistemas Borrosos 3 Ed Benifacio Martin Del Brio Alfredo Sanz Molina. Retrieved February 25, 2019, from https://www.scribd.com/document/361136011/Redes-Neuronales-y-Sistemas-Borrosos-3-Ed-Benifacio-Martin-Del-Brio-Alfredo-Sanz-Molina

Deloitte. (2017). Global risk management survey, 10th edition | Deloitte Insights. Retrieved March 1, 2019, from https://www2.deloitte.com/insights/us/en/topics/risk-management/global-risk-management-survey.html

Demirel, T., Demirel, N. Ç., & Kahraman, C. (2008). Fuzzy Analytic Hierarchy Process and its Application (pp. 53–83). Springer, Boston, MA. https://doi.org/10.1007/978-0-387-76813-7_3

Duch, W. (2007). *What is Computational Intelligence and what could it become?* Retrieved from http://cogprints.org/5358/1/06-CIdef.pdf

Embrechts, P., Hansj¨, H., Furrer, H., & Kaufmann, R. (n.d.). *QUANTIFYING REGULATORY CAPITAL FOR OPERATIONAL RISK*. Retrieved from https://www.bis.org/bcbs/cp3/embfurkau.pdf

Erensal, Y. C., Öncan, T., & Demircan, M. L. (2006). Determining key capabilities in technology management using fuzzy analytic hierarchy process: A case study of Turkey. *Information Sciences*, *176*(18), 2755–2770. https://doi.org/10.1016/j.ins.2005.11.004

Estivill-Castro, V. (2002). Why so many clustering algorithms. *ACM SIGKDD Explorations Newsletter*, *4*(1), 65–75. https://doi.org/10.1145/568574.568575

EY. (2014). *Identifying ways to get ahead of cybercrime Insights on governance, risk and compliance Cyber program management*. Retrieved from https://www.ey.com/Publication/vwLUAssets/EY-cyber-program-management/$FILE/EY-cyber-program-management.pdf

Health Service Executive. (2011). *Risk Assessment Tool and Guidance*.

Hsu, W.-K. K., Huang, S.-H. S., & Tseng, W.-J. (2016). Evaluating the risk of operational safety for dangerous goods in airfreights – A revised risk matrix based on fuzzy AHP. *Transportation Research Part D: Transport and Environment*, *48*, 235–247. https://doi.org/10.1016/j.trd.2016.08.018

IACOB, V.-S. (2014). *RISK MANAGEMENT AND EVALUATION AND QUALITATIVE METHOD WITHIN THE PROJECTS*. *Ecoforum Journal* (Vol. 3). Retrieved from http://ecoforumjournal.ro/index.php/eco/article/view/58

ISO/IEC 2018. (2018). *Information technology-Security techniques-Information security risk management*. Retrieved from www.iso.org

ISO. (2009). ISO/Guide 73:2009(en), Risk management — Vocabulary. Retrieved August 3, 2017, from https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en

Jan Duijm Duijm, N., & Jan, N. (2015). *Recommendations on the use and design of risk matrices*. Retrieved from www.man.dtu.dk

Jiménez Rodríguez, E. J., Feria Domínguez, J. M., & Martín Marin, J. L. (n.d.). STRESSING THE OPERATIONAL LOSS THRESHOLD: IMPLICATIONS ON CAPITAL AT RISK. Retrieved from http://www.efmaefm.org/0EFMAMEETINGS/EFMA ANNUAL MEETINGS/2010-Aarhus old/EFMA2010_0118_fullpaper.pdf

Kulak, O., Durmuşoğlu, M. B., & Kahraman, C. (2005). Fuzzy multi-attribute equipment selection based on information axiom. *Journal of Materials Processing Technology*, *169*(3), 337–345. https://doi.org/10.1016/j.jmatprotec.2005.03.030

Levine, E. S. (2012). Improving risk matrices: the advantages of logarithmically

scaled axes. *Journal of Risk Research*, *15*(2), 209–222. https://doi.org/10.1080/13669877.2011.634514

Lu, L., Liang, W., Zhang, L., Zhang, H., Lu, Z., & Shan, J. (2015). A comprehensive risk evaluation method for natural gas pipelines by combining a risk matrix with a bow-tie model. *Journal of Natural Gas Science and Engineering*, *25*, 124–133. https://doi.org/10.1016/j.jngse.2015.04.029

Markowski, A. S., & Mannan, M. S. (2008). Fuzzy risk matrix. *Journal of Hazardous Materials*, *159*(1), 152–157. https://doi.org/10.1016/j.jhazmat.2008.03.055

McNeil, A. J., Frey, R., & Embrechts, P. (2015). *Quantitative risk management : concepts, techniques and tools*. Princeton University Press.

Microsoft. (2019). Choosing the best trendline for your data. Retrieved May 8, 2019, from https://support.office.com/en-ie/article/choosing-the-best-trendline-for-your-data-1bb3c9e7-0280-45b5-9ab0-d0c93161daa8

Mitchell, T. M. (1997). *Machine Learning*. Retrieved from http://profsite.um.ac.ir/~monsefi/machine-learning/pdf/Machine-Learning-Tom-Mitchell.pdf

Mora, J. A. N., & Gudiño, J. J. C. (2010). Riesgo operativo: esquema de gestión y modelado del riesgo. Retrieved from https://redalyc.org/articulo.oa?id=41313083007

Mu, E., & Pereyra-Rojas, M. (2017). Understanding the Analytic Hierarchy Process (pp. 7–22). Springer, Cham. https://doi.org/10.1007/978-3-319-33861-3_2

National Patient Agent Safety. (2008). NRLS | 0676 | A risk matrix for risk managers. Retrieved from http://www.nrls.npsa.nhs.uk/EasySiteWeb/getresource.axd?AssetID=60149

Navarrete, E. (2006). Practical Calculation of Expected and Unexpected Losses in Operational Risk by Simulation Methods. Retrieved from https://www.palisade.com/downloads/pdf/CalculationofExpectedandUnexpectedLossesinOperationalRisk.pdf

Peña, A., Lochmuller, C., & Patiño, A. (n.d.). Computational Intelligence Toolbox.

Peters, J. F. (2009). Fuzzy Sets, Near Sets, and Rough Sets for Your Computational Intelligence Toolbox (pp. 3–25). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-01533-5_1

Ramakrishnan, N. (2009). *The Top Ten Algorithms in Data Mining*. Retrieved from https://doc.lagout.org/Others/Data Mining/The Top Ten Algorithms in Data Mining %5BWu %26 Kumar 2009-04-09%5D.pdf

Rohmeyer, P., & Bayuk, J. L. (2019). *Financial Cybersecurity Risk Management*. Berkeley, CA: Apress. https://doi.org/10.1007/978-1-4842-4194-3

RSA. (2016). *CYBER RISK APPETITE: Defining and Understanding Risk in the*

Modern Enterprise. Retrieved from http://www.reuters.com/article/us-nasdaq-halt-glitch-idUSBRE97S11420130829

Sadhana, C., & Shanmugapriya, S. (2017). Assessment of Risk in Construction Projects by Modified Fuzzy Analytic Hierarchy Process, *4*(3). Retrieved from https://www.irjet.net/archives/V4/i3/IRJET-V4I3390.pdf

Siddique, N., & Adeli, H. (2013). *Computational Intelligence : Synergies of Fuzzy Logic, Neural Networks and Evolutionary Computing.* Wiley. Retrieved from https://www.wiley.com/en-us/Computational+Intelligence%3A+Synergies+of+Fuzzy+Logic%2C+Neural+Networks+and+Evolutionary+Computing+-p-9781118337844

Superintendencia Financiera de Colombia. (2006). REGLAS RELATIVAS A LA ADMINISTRACIÓN DEL RIESGO OPERATIVO. In *Circular Externa 048 de 2006* (p. 10). Retrieved from https://www.superfinanciera.gov.co/SFCant/NormativaFinanciera/Archivos/ance048_06.rtf.

The MathWorks, I. (2019a). Fit probability distribution object to data - MATLAB fitdist. Retrieved April 22, 2019, from https://www.mathworks.com/help/stats/fitdist.html

The MathWorks, I. (2019b). Model Data Using the Distribution Fitter App - MATLAB. Retrieved April 22, 2019, from https://www.mathworks.com/help/stats/model-data-using-the-distribution-fitting-tool.html

Valová, I. (2011). *BASEL II APPROACHES FOR THE CALCULATION OF THE REGULATORY CAPITAL FOR OPERATIONAL RISK*. Retrieved from http://www.cnb.cz.

Verizon. (2018). *2018 Data Breach Investigations Report 11 th edition*. Retrieved from http://bfy.tw/HJvH

Vilaragut, J. J., Duménigo, C., Delgado, J. M., Morales, J., McDonnell, J. D., Ferro, R., … Nader, A. (2013). Prevention of Accidental Exposure in Radiotherapy. *Health Physics*, *104*(2), 139–150. https://doi.org/10.1097/HP.0b013e3182680379

Wang, X., Chan, H. K., Yee, R. W. Y., & Diaz-Rainey, I. (2012). A two-stage fuzzy-AHP model for risk assessment of implementing green initiatives in the fashion supply chain. *International Journal of Production Economics*, *135*(2), 595–606. https://doi.org/10.1016/j.ijpe.2011.03.021

Wind, Y., & Saaty, T. L. (1980). Marketing Applications of the Analytic Hierarchy Process. *Management Science*, *26*(7), 641–658. https://doi.org/10.1287/mnsc.26.7.641

Wu, J. (2012). Cluster Analysis and K-means Clustering: An Introduction (pp. 1–16). https://doi.org/10.1007/978-3-642-29807-3_1

Zhou, Q., & Thai, V. V. (2016). Fuzzy and grey theories in failure mode and effect analysis for tanker equipment failure prediction. *Safety Science*, *83*, 74–79.

https://doi.org/10.1016/J.SSCI.2015.11.013