THE JOURNAL OF COMPUTER SCIENCE AND ITS APPLICATIONS
Vol. 27, No. 2 December 2020

A FUZZY LOGIC RISK CONTROL AND SELF-ASSESSMENT METRICS FOR e-BANKING OPERATIONAL RISK ANALYSIS

[1] Ako, R. E., [2] Oghorodi, D. and [3] Okpako, A. E.
[1,3]Department of Mathematical Sciences Edwin Clark University, Kiagbodo Delta State, Nigeria
[2]Department of Computer Science, College of Education, Warri, Delta State, Nigeria
[1]ochukorita2@gmail.com [2] dukeoghorodi@gmail.com [3] okpako.ejaita@gmail.com
Corresponding Author: ochukorita2@gmail.com

ABSTRACT

Operational risk is the risk of losses arising from the failure or inadequate internal processes, human resources, systems, and external events that affect the bank's operations as defined by Basel Committee on Banking Supervision. Defining a suitable set of risk measurement metrics is considered one of the most important issues for any risk analysis. It enables the quantitative evaluation of the risk exposure level and the effectiveness of internal control system. Risk measurement is needed to provide an effective means to quantify the risk of existing or planned systems to enable understanding of the overall security level and to guide decision making. Given the number of successful attacks against financial Institutions and the sophistication of the tactics used by attackers, existing classical measurement approaches are no longer enough. This study focuses on fuzzy logic-based metric identification to measurement of the risk exposure level, to enable financial institutions to see the overall risk level and security state of their E-banking systems and to assist with decision making. This will provide a newer dimension to risk management by shifting from risk measurement based on probability and classical set theory to Fuzzy Logic (FL) measurement. In this paper fuzzy logic-based metrics is presented and expressed as a function of six factors (triggering events, avoidance, recovery, Undesirable Operational State (UOS), cost of Undesirable Operational State (UOS) occurrence and severity of risk occurrence) as proposed by [1].

Keywords: Risk Assessment, Operational Risk, Fuzzy Logic.

1.0 INTRODUCTION

1.0 Introduction

The Basel Committee on Banking Supervision [9], described Risk Assessment as a Risk Self-Assessment (RSA), where a bank assesses the processes underlying its operations against the potential threats, vulnerabilities, and their potential impact, which will help in revealing the risk exposure level and the security posture in the context domain. Similarly Risk Control Self Assessments (RCSA) is evaluated by taking into consideration inherent risks and the effectiveness of the control environment, which help to identify the residual risks [4]. RCSA can be done through mapping processes, brainstorming sessions, surveys,

and assessments from Special Matter Expertise (SME) or interviews.

Risk analysis refers to a process of estimating the frequency and physical consequences of undesirable events [24]. It is a systematic description and evaluation of risk, which involves identifying undesirable risk events, their triggering events and consequences of these risk events, taking into consideration the effectiveness of existing or planned controls [16]. The resulting consequences and their probabilities are then calculated to determine the risk exposure level. Risk analysis can therefore be defined as a process to assist management in defining where time, money, and improvement should be made on the overall business or operations [15, 17]. The traditional approach to risk analysis is to apply an impact and likelihood matrix which provides an overall risk rating [16, 221, 22, and 23]. Many risks are however subjective and qualitative, rather than objective, identifiable and measurable risks. For example, the risks of litigation, economic downturn, loss of key employees, natural disasters and loss of reputation are all subjective judgments. One of the issues is that traditional risk assessment techniques often focuses on those elements that can be quantified easily. Such techniques fail to address all critical drivers of successful risk management [19]. Various approaches may be used to assess the severity and likelihood of each risk once it has been identified. The definition of what these attributes mean and how they are employed in the risk analysis process differs between researchers and organizations. There is no consensus on the best approach to implementing self-assessment [23].

Defining a suitable set of risk measurement metrics is considered to be one of the most important issues for any risk analysis process; this enables the quantitative evaluation of the risk exposure level and the effectiveness of internal control system, which supports the foundation for decision making on risk mitigation [3]. This study focuses on the metric definition to quantify the risk exposure level. A Risk Control and Self-Assessment (RCSA) metrics approach and a threat-oriented metrics approach were used; the level of risk depends on the adequacy and effectiveness of existing controls [19].

This paper outlined an E-banking operational risk management framework for effective operational risk exposure determination, providing decision makers with important information on the level of success in meeting organization's objectives. It provides metrics for risk and control self-assessment that harmonizes and resolves the differences between currently accepted qualitative and quantitative RCSA methodologies and uncover the inherent risk exposure within business processes.

This paper focuses on the application of fuzzy logic and fuzzy set theory, introduced by mathematician, Lotfi A. Zadeh in 1965 to E-banking operational risk assessment. In this paper, fuzzy logic was used to simulate the subjective process of normal human reasoning and represent fuzzy truth membership in vaguely defined sets by trying to answer questions such as: what is the likelihood (estimated frequency) of triggering threat events, the likelihood (frequency) of Undesirable Operational State (UOS) occurrence, the effectiveness of controls in place to avoid and recover before the operational risk outcome, the estimated cost of UOS and the severity of operational risk outcome. The determination of risks for E-banking OR is expressed as a function of the six factors (triggering events, avoidance, recovery, UOS, cost of UOS occurrence and severity of risk occurrence).

2.0 LITERATURE REVIEW AND RELATED WORK

Measuring the uncertainty in a risk exposure refers to the explicit quantification of

probabilities and potential consequences based on all the information available about risks under consideration. The measurement of operational risks in most banks is at early stages with only a few of them having formal measuring procedures in place. The Basel Committee noted also that while most banks have established a risk self-assessment, or a Risk and Control Self-Assessment (RCSA), many indicated that the tool has not yet been fully implemented or was currently undergoing some form of change or enhancement [10]. More specifically, fewer than half the number of banks indicated that the RCSA was implemented on an enterprise-wide basis. There also appears to be a very wide range of practice as to the design and implementation of these tools [10].

[25] implemented a RCSA using Rapid Application Development model in bank operational risk management process to ascertain the application of Risk Control Self-Assessment (RCSA) to measure operational risk, with the possibility of frequency dimensions and the magnitude of the impact that may occur while implementing operational risk controls to remain within the acceptable operational risk tolerance level and to improve the risk awareness culture through monitoring of the level of effectiveness of the risk controls that have been carried out and determining the priority scale of corrective actions. In their Rapid Application Development model, they built an operational risk assessment (*frequency and impact*) matrix with a 5 scale likelihood categories of "*Almost Certain to Rare*" rating. The control testing method in each working unit was conducted by testing controls for inherent risks with "*Moderate, Moderate to High, and High*" rank level. The final results that are expected with the implementation of the Risk Control Self-Assessment (RCSA), is the improvement of risk consolidation after risk mitigation.

[2] opined that risk analysis should be developed to understand the level of the risk or risk score, the underlying causes and the existing control measures. Risk score is calculated by multiplying the likelihood score with the severity of impact score. A classical risk formula i.e. *severity x likelihood* equals the *risk score*. Likelihood scoring is based on the expertise, knowledge and actual experience of the group scoring the likelihood. Risks are assessed on the probability of future occurrence; how likely is the risk to occur? How frequently has this occurred? The assessment of likelihood of a risk occurring is assigned a number from 1-5, with 1 indicating that there is a remote possibility of its occurring and 5 indicating that it is almost certain to occur. Severity of impact on the other hand indicates the impact of harm to service users, employees, service provision, environment or the organization. The scoring ranges from 1 (Negligible impact) to 5 (Extreme impact).

Risk score (R) = *Likelihood (L)* x *Severity of impact (S)* …… (1)

The risk score is calculated on a scale of 1-25, with 1-5 classified as low risk, with 6-12 as medium risk while 15-25 as high risk.

[19] developed a risk quantification matrix and a risk register form to identify potential risks in the operating room, and implemented operating room policies designed to reduce or eliminate those risks. The consequences of 10 risks were analyzed in the Risk Register by using a two dimensional Risk quantification matrix. The consequence analyses for the identified risks from the risk register were divided into categories of insignificant (category 1), minor (category 2), moderate (category 3), major (category 4), and extreme (category 5), based on their seriousness and potential costs. The likelihood that a risk event will actually occur is also described in a 5 level format. The probability of occurrence is divided into categories of remote (1), unlikely (2), possible (3), likely (4) and almost certain (5). The overall risk associated with an event is

then calculated by multiplying the consequence score by the likelihood score. When using this process, scores of 1-5, 6-15, and >16 signify low, moderate and major risks, respectively.

[4] developed a comprehensive risk and control self-assessment methodology and an associated scenario analysis approach. They introduced a practical, proactive, robust risk management model and metric for risk and control self-assessment (RCSA) that harmonizes and resolves the differences between currently accepted qualitative and quantitative RSCA methodologies. Their metric also preserves management's ability to uncover risk exposures inherent within business processes and monitor the residual risks the firm is willing to accept. They define the qualitative terms for describing the observed levels of risk exposure; these are the *risk assessment* and *control effectiveness* scales. The RCSA risk exposures were ranked as 'low', 'medium', or 'high' and converted quantitatively within the RCSA metric. They opined that the risk manager must first decides on the number of tiers (3 or 5) to illustrate *riskiness* – that is, the 'levels' needed to describe the range from *low* to *high* risk. Similar to the rating scale, the risk manager assigns consistent frequency and severity scale descriptions. The frequency and severity descriptors are two and six perspectives. The frequency risk scale is define by "*Occurrence and Percentage*" while the evaluation of the severity scale definition is by "*Financial, People, Process, Technology, Relationship and Regulatory*". A scale of categories must also be adopted for appraising control activities (risk mitigants) from "*least effective to most effective*". However for logical consistency, the number of categories in the control effectiveness scale should always match the number of levels used for the frequency and severity assessment scales. The first step in defining control effectiveness categories is defining the *control effectiveness criteria*, which are the qualitative judgments used to assess the controls. Each of these criteria is assigned a *control effectiveness range* ($0 \leq \alpha \leq 1$), which complements the criteria and helps the manager determine the appropriate category by reflecting how well a control is working. The control effectiveness range is also the starting point for quantifying the subjective control effectiveness assessment. Lastly, the mid-point of the control effectiveness range becomes the calculation value used in the RCSA metric model.

3.0 ANALYSIS OF EXISTING RISK CONTROL SELF-ASSESSMENT METRICS

According to [2]) *Probability* is the measure of the likelihood that an event will occur. *Threat* is any activity that represents a possible danger. *Vulnerability* is a weakness. *Loss* results in a compromise to functions, life or assets. *Incident* is an undesired outcome or occurrence, not expected within the normal course of care or treatment, disease process, condition of the patient, or delivery of services. Risk analysis is about developing an understanding of the risks identified. It includes the level of the risk or risk score, underlying causes and existing control measures.

A detailed review of existing risk analysis metrics was carried out in order to bring to the fore areas to improve on in order to tackle problem of subjectivity and uncertainty in risk analysis process and specifically E-banking OR measurement metrics. Classical risk score is calculated by multiplying the likelihood score with the severity of impact score as stated in equation 1 above. Several researchers have applied these classical risk analysis approaches to measuring risks and from the analysis of the literature a major limitation or drawback is that Boolean or conventional logic which uses sharp distinctions [0-1] has been proposed. This logic forces the risk analyst to

draw lines between members of a class and non-members. For instance the scores of 1-5, 6-15, and >16 would signify low, moderate and major risks, respectively. By this standard scores that can cover between 5 and 6, 15 and 16 would not be classified. There is also no room for over lapping classification as seen in real life human-like subjective judgment.

The [4] RCSA measurement metrics, the British Standards Institution, (2010) and the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0 (2007) were considered. Interestingly, in these studies it was found that there was no general consensus on used risk measurement metrics. Two common risk analysis attributes (frequency of occurrence and severity of impact estimation) were used. However our focus is on the [4] RCSA measurement metrics. The Alvarez & Gledhill RCSA metrics has the ability of significantly shifting from classical risk measurement methods to a new risk measurement method by introducing a practical, proactive, robust risk metric and control self-assessment (RCSA).

4.0 DESIGN OF THE PROPOSED FUZZY LOGIC RISK CONTROL SELF-ASSESSMENT METRICS

Defining a suitable set of measurement metrics for the risk analysis process enables the quantitative evaluation of the risk exposure levels and the effectiveness of internal controls. We reviewed a Risk Control and Self-Assessment (RCSA) metrics approach and a threat-oriented metrics approach [6,7,13] in order to solve the challenges brought by the subjective nature of risk measurements and represent the results in an informative and intuitive manner by addressing questions such as:

i. What is the frequency (likelihood) of triggering events?
ii. What is the frequency (likelihood) of UOS occurrence?
iii. What are the existing controls for the identified risk issues?
iv. Were those controls capable of adequately avoiding or recovering the risk events before the risk outcome?
v. In practice, did the controls operate in the manner intended and demonstrated effective when required?
vi. What is the severity (impact) of risk outcome?

4.1 Measurement and Metrics Definition

In this study, we proposed an integration of the RCSA, threat-oriented and FL approaches to obtain the risk assessment metrics, measure the risk exposure level, and determine the security level within an E-banking OR system. These measurements are based on the function of the six factors. The results obtained for measurement metrics of the six factors are presented in Tables 1 to 6. The RCSA approach is based upon the assumption that, to transparently identify and assess the bank's risk exposures and gauge the strength of the control activities in place, objective criteria to assess the risks and controls must be specified. To achieve this, a rigorous RCSA metrics and qualitative terms for describing the observed levels of risk exposure was defined. The RCSA process is depicted in Figure 1.

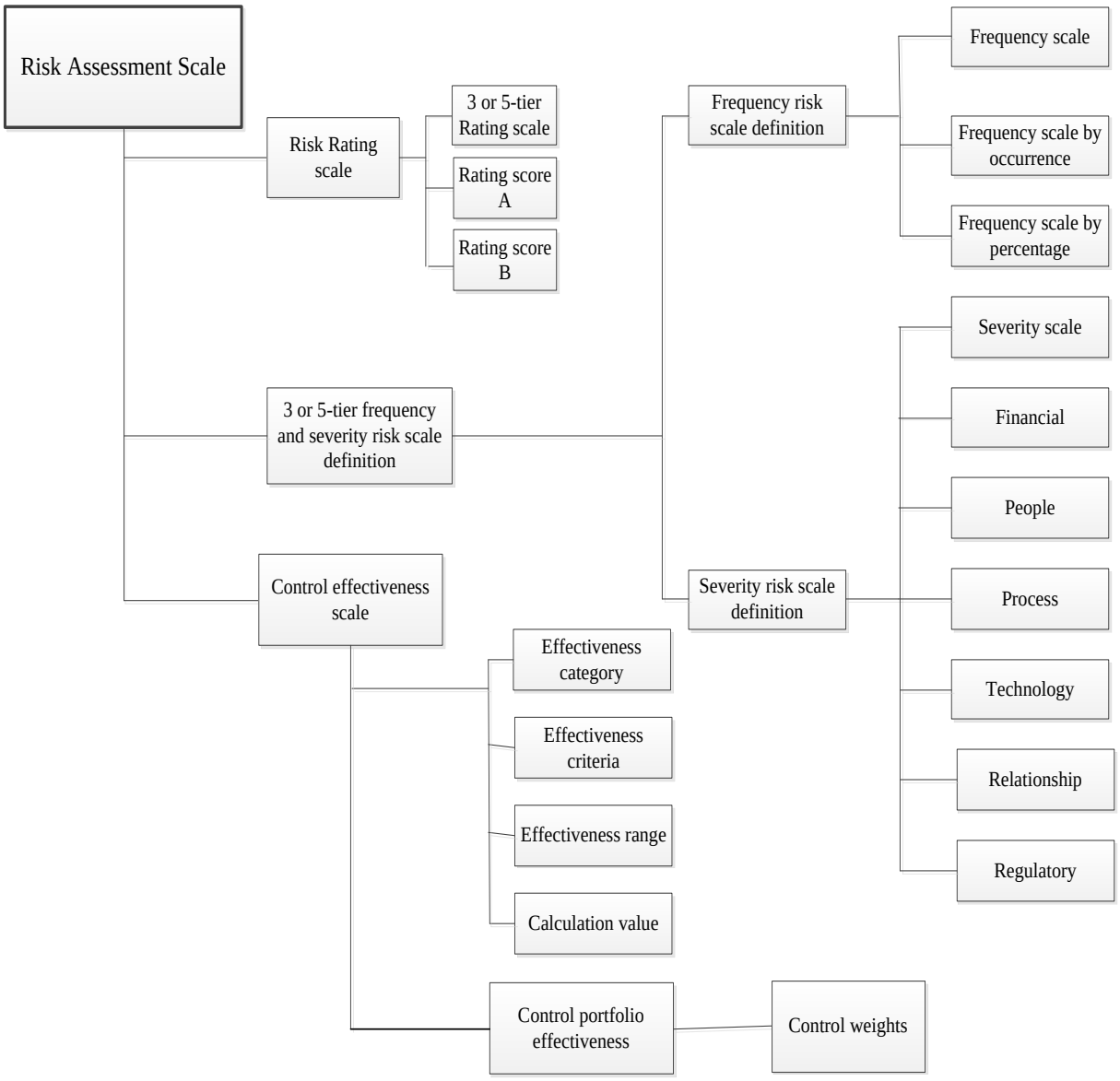

Figure 1: The graphical structure of the RCSA process

By using the RCSA approach, many current approaches can be combined to measure the E-banking OR exposure level; these include the ARMS working group (2010) and the NIST SP 800-30 revision 1 (2011) risk assessment approaches.

– **The risk rating scale description:** Consistent risk rating scale should be defined for frequency and severity in this level. The risk analysts must first decide on the number of tiers to illustrate the riskiness - that is using either a 3-tier (*low, medium, and high*) or a 5-tier (*very low*, *low*, *medium, high and very high*) to describe the range of risk.

– **The frequency and severity scale description:** Using a 3 or 5-tier scale, the risk analysts should define frequency and severity descriptors consistent with the needs of the organization in this level. There are three perspectives to consider when evaluating the frequency and seven

perspectives when evaluating severity of the risk as indicated in Table 1 below.

Table 1: Frequency risk scale definition

Qualitative values	Semi-quantitative values		Trapezoidal Fuzzy numbers	By number of occurrence	By percentage
Very frequent	80-100	10	[0.6, 0.9, 1, 1]	Occurrence of a TE or UOS is one or more monthly	Occurrence of a TE or UOS is >50% of transactions
Occasionally	21-79	5	[0.3, 0.4, 0.6, 0.7]	Occurrence of a TE or UOS is2 to 3 times within the calendar/fiscal year	Occurrence of a TE or UOS is > 30% and <50% of transactions
Very rarely	0-20	0	[0, 0, 0.2, 0.4]	Occurrence of a TE or UOS is<once during a calendar/fiscal year	Occurrence of an event is <10% and < 30% of transactions

– **Control effectiveness scale description: A** scale of categories should be defined for assessing control activities from "*least effective to most effective*". For logical consistency the number of categories in the control effectiveness scale should match the number of levels used for frequency and severity assessment scales. There are four perspectives to consider when evaluating the control effectiveness: control effectiveness category, control effectiveness criteria, range and calculation value. However, organizations usually implements more than one control activity to manage a risk, thus a portfolio of controls should be used to determine the contributions made by the individual controls to the overall portfolio's effectiveness (the control 'weights'). All controls in the portfolio should either be weighted equally or have specific weights.

4.1.1 Frequency and Severity Scale Definition

The starting point to creating the RCSA and the threat-oriented metrics is to identify both qualitative and semi-quantitative values for the frequency of triggering events, frequency of UOS occurrence and severity of the risk. Determining the frequency (likelihood) is fairly straightforward. It is the occurrence or percentage count of an UOS and a triggering event (e.g. threats, threats agent exploiting vulnerabilities, key risk indicators or other attributes). Severity of risk on the other hand is the process of determining the impact upon Confidentiality, Integrity and Availability (i.e. the CIA triad) when a risk is successfully executed. This process helps the risk analysts to focus on not only the financial impact of the risk exposure, but also on other important dynamics that could impede the achievement of the business objectives such as an adverse regulatory action, a process disruption or incapacitation of a critical infrastructure.

However, risk analysts often rely on common sense when conducting risk analyses for such complex systems. They often use vague and qualitative terms such as "*very high", "high", "average", "low" and "very low"* (also known as linguistic values), in dealing with uncertain factors within complex systems. Fuzzy logic can incorporate expert qualitative judgement to define those variables and their relationships. The example of a 3-tier frequency scale

definitions, the severity scale and definitions for the risk categories used in evaluating the severity risk outcome is presented in Table 1, 2, and 3 respectively for the E-banking ORA. At the end of this step, a set of fuzzy risk scales and scales description is provided.

The frequency of triggering events is quantitatively defined to assessing an individual triggering event. Usually various events can trigger a given risk event within a business process. The individual triggering event must be aggregated into a portfolio of triggering events. One simplified approach is treating the triggering events as one. Though this methods seems easy to use, the risk assessment granularity will however be sacrificed. Thus a more detail approach is to average the individual triggering events. The generalized expression for the aggregate triggering events is:

$$TE_{RP} = \frac{\sum_{i=1}^{n} F_{te_i}}{N_{te}} \qquad \text{……Eq (2)}$$

where te = triggering events, N_{te} = Number of triggering events, and F_{te_i} = frequency of triggering events.

Tables 2 and 3, defines the severity risk scale.

Table 2: Definitions for risk categories used in evaluating severity component of risk

Severity descriptors	**Definitions**
Total Financial cost	The risk of a loss (including the cost of UOS and other perspectives described in the risk scale definition) that is readily quantifiable and has an accounting and / or economic impact on the firm. It may be outsider or insider attacks
People	The risk intentionally or unintentionally caused by an employee (through error or misdeed) or involving employees, such as in employment disputes. This covers internal organisational problems, people risks arise from the action or inaction of an individual or a small group of people within the firm.
Process	The risks related to execution and maintenance of transactions, and the various aspects of running a business, including products and activities. Process risks are problems that are systematic in an institution or group, or inherent in a business process.
Technology	The risk caused by privacy, theft, failure, breakdown or other disruption in technology, data or information; also includes technology that fails to meet business needs. Technology risks can occur in any department; not just those that manage the firm's E-banking infrastructure.
Relationship	The risk arising from the relationships or contact a firm has with its customers, shareholders, stakeholders or counterparties. Relationship risks include a human element but they are distinct from people risk incidents because they are based on the interaction between the firm and outside entities or, in some cases, the connection among groups within the firm.
Regulatory	The risk associated with the firm not complying with regulations, law or supervisory guidance.

Table 3: Severity risk scale definition

Qualitative values	Semi-quantitative values		Trapezoidal Fuzzy numbers	Financial cost	People	Process	Technology	Relationship	Regulatory
Extremely severe	80 - 100	10	[0.7, 0.9, 1, 1]	[>1m]	Employee commits a legal and / or regulatory wrongful act Employee suffers an injury that results in health and / or personal safety issue	Process does not execute Process needs to execute its business resiliency plan	Complete failure in service Interruption resulting in big impact to business	Third party experiences complete disruption to its business	Regulator closes or takes over business Regulatory criticism fine, and curtailment of business
Moderately severe	21 - 79	5	[0.3, 0.4, 0.6, 0.9]	[500k, 1m]	Employee's performance and / or behaviour requires management action up to and including dismissal Employee suffers discrimination and / or harassment issue	Process is delayed due to disruption or re-work performed No business impact despite minimal disruption	Performance interruption and impact to business (e.g. delay in process or re-work) Performance interruption but no impact to business	Third party experiences minor disruption to its business and inconvenience	Regulatory criticism and fine
Not at all severe	0 - 20	0	[0, 0, 0.2, 0.4]	< 500k	Employee's performance does not negatively affect the firm	No disruption	No performance interruption	Third party experiences no impact	No regulatory impact

4.1.2 Barriers/Control Failure Scale Definition

In order to quantify the effectiveness of controls in the E-banking system, the scale for effectiveness of controls to avoid UOS and recover before risk outcome must be defined, from "*practically always failing* to *very rarely failing*" categories. When conducting the business or functional unit's activities, the qualitative control failure criteria are defined. Each of these criteria is assigned a control failure range to complement the criteria and help the risk analysts in determining the appropriate category while looking at the control effectiveness. Control failure range is however the starting point for quantifying the subjective control failure assessment. Lastly the mid-point of the control failure range is the calculation value used. Table 4 list three control failure categories, qualitative control failure criteria for each, the control failure ranges, and the subsequent calculation values. However, as mentioned earlier risk analysts often use vague and qualitative terms when conducting risk analyses, as a

result a Fuzzy Logic risk scale, which is able to incorporate effectively experts' qualitative judgments to define those variables and their relationships is defined.

Up to this point, the control effectiveness scale is quantitatively defined to assessing an individual control. Usually organizations implements more than one control activity to manage risk exposures. The individual control effectiveness must be aggregated into a portfolio of controls. To address the situation, risk analysts must resolve one unknown, determining the contributions made by the individual controls to the overall portfolio of control (the control 'weights'). There are two general conditions to assigning weight: all of the controls in the portfolio are either equally weighted or they have specific weights. Equally weighted controls contribute equally to the portfolio of controls, whereas controls with specific weights contribute to the portfolio by prescribed amounts. Regardless of the weight chosen, portfolio of controls (α_{cp}) can be quantified as:

$$\alpha_{cp} = \sum_{i=1}^{n} \alpha_i \omega_i \qquad (3)$$

Where α_i the individual are control effectiveness values, and ω_i are the control weights. In this study the control weights must sum to 1 as shown below:

$$\sum_{i=1}^{n} \omega_i = 1 \qquad (4)$$

Table 4: Control failure scale for (barriers to avoid UOS and recover before the risk outcome)

Control Failure category	Control Failure criteria	Control Failure range	Calculation value	Trapezoid Fuzzy numbers
Practically always	• Control objective is able to mitigate risk exposure(s) • Controls portfolio denies or delay unauthorized access to the E-banking system • Barriers is able to prevent or detect malicious transaction or malwares • Control portfolio is executed as designed • No significant gap in controls design and execution • Control portfolio did recover before the risk outcome	70% - 100% ($0.7 \leq \alpha \leq 1$)	95%	[0.7, 0.9, 1, 1]
Sometimes	• Controls objective somewhat mitigate risk exposure • Controls portfolio did not completely deny or delay unauthorized access to the E-banking system • Barriers is primarily detective of malicious transaction or malwares • Control portfolio is reasonably executed as designed • Significant gap in controls design and execution • Control portfolio did not always recover before the risk outcome	50% - 70% ($0.5 \leq \alpha < 0.7$)	60%	[0.3, 0.4, 0.6, 0.9]
Very rarely	• No controls in place to prevent or recover before risk outcome • Controls portfolio did not deny or delay unauthorized access to the E-banking system • Barriers did not detect malicious transaction or malwares • Control portfolio is irregularly executed as designed • Significant gap in controls design and execution	0% - 30% ($0 \leq \alpha < 0.5$)	15%	[0, 0, 0.2, 0.4]

Although, equation (3) and (4) are straightforward, risk analysts may find it difficult to assign individual weights for each control activity in the control portfolio. This can however be avoided by assigning qualitative categories such as 'primary', 'secondary', and 'tertiary', or numerical ranking such as 1st, 2nd and 3rd to characterise control weights. The use of control weight categories will enable consistency across organization (Alvarez and Gledhill, 2010).

4.1.3 Cost of UOS Scale Definition

In order to quantify the cost for UOS occurrence, the risk scenario must first be defined. Risk or threat scenario may be described in terms of loss of data or system integrity, loss of availability and loss of confidentiality. For example, an attacker (insider or outsider) pretended to be a legitimate mobile banking agent because he/ she was able to gain unauthorized access to the mobile banking agent system and gained access to the agent login IDs. He then uses the stolen details to masquerade in order to steal customers' money. For this reason, the UOS is loss of data integrity through account comprise, which must in turn be assigned an estimated cost for occurrence. Determining the approximate cost of UOS is fairly straightforward, it is the quantitative value for an UOS occurrence using the environment upon which the UOS is situated. This will help the risk analysts in identifying more clearly the magnitude of impact and the risk exposure levels. Table 5 lists the qualitative and quantitative values, the trapezoidal fuzzy numbers and the definition. Looking at Table 5 for instance, an approximate cost of UOS scale could be defined as the loss to data or system integrity, as a result of unauthorized changes on the E-banking system, leading to account compromise or theft is "very high" and is under the quantitative values greater than £1,000,000.00.

Table 5: Approximate cost of UOS definition

Qualitative values	Quantitative values	Trapezoid fuzzy numbers	Definition
Very high	[≥ 1m]	[0.7, 0.9, 1, 1]	• Loss to data or system integrity: unauthorized changes had been made to the data or E-banking system, leading to account compromise, fraud, identity theft, or erroneous decisions. • Loss of availability: mission critical to the E-banking system is unavailable to the customers and the organization's mission is affected, leading to loss of productive time and delays in transaction processing. • Loss of confidentiality: unauthorized disclosure of confidential information and data, leading to jeopardizing privacy and identity theft. As result the organization suffers lack of public confidence, embarrassment, or legal actions.
Average	[5k, 1m]	[0.3, 0.4, 0.6, 0.9]	
Very low	< 5k	[0, 0, 0.2, 0.4]	

4.1.4 Risk Exposure Level Scale Definition

Assessing the E-banking OR is a combination of likelihood, impact and cost results. Likelihood, impact and cost are assessed on the system as it is operating at the time of the assessment. The level of risk associated with identified risk represent a determination of the degree to which organizations are threatened by such risk issues. Equation (5) reveals that risk exposure level is simply the product of the ORA factors once they are assessed.

$$\mathrm{Re}l_{x_i} = F_{te} \times FA_{uos} \times F_{uos} \times F_{rr} \times EC_{uos} \times S_{ro} \quad \ldots\ldots\ldots\ldots(5)$$

Where Rel = risk exposure level, F_{te} = frequency of triggering events, FA_{uos} = failure to avoid UOS, F_{uos} = frequency of UOS occurrence, F_{rr} = failure to recover before risk outcome, EC_{uos} = estimated cost of UOS, S_{ro} = severity of risk outcome.

Table 6: Risk Exposure level scale

Qualitative values	Quantitative values	Trapezoidal fuzzy numbers ($TrFN_L$)	Definition
Very low risk	[10 – 40 %]	[0, 0, 0.2, 0.4]	• The organization will accept these levels of risk since they have small or negligible impact on the E-banking system.
Medium risk	[35 - 65%]	[0.3, 0.4, 0.6, 0.7]	• The organization will accept these levels of risk since they could have a very noticeable impact on the E- banking system, which needs to be monitored and / or dealt with as appropriate.
Very high risk	[60 – 100%]	[0.6, 0.9,1.0,1.0]	• The organization will accept these levels of risk since they could have a very serious and critical impact on the business, which needs urgent and immediate attention.

When determining risk at 100% probability of certainty, it is consistent that the risk level equals the impact level [22]. Each risk corresponds to a specific risk issue with a level of impact if those issues were exploited. In general, a risk level is typically not higher than the impact level. However, when addressing the portfolio of risk (such as in E-banking systems), this upper bound assumption may not hold, due to the potential aggregation of risk. To address the situation, risk analysts must resolve one unknown: determining the contributions made by the individual risk to the overall portfolio of risk (averaging the individual risk). The general expression for aggregation of risk is:

$$Rel_{RP} = \frac{\sum_{i=1}^{n} F_{te} \times FA_{uos} \times F_{uos} \times F_{rr} \times EC_{uos} \times S_{ro}}{Number\ of\ risks} \quad (6)$$

where Rel_{x_i} is the mean value for the collection of risk exposures. Hence equation (6) will yield the result for a portfolio of risk exposure level for the E-banking OR. Table 6 list both qualitative and quantitative values, the trapezoidal fuzzy numbers and definitions adopted in this research.

5.0 CONCLUSION AND FUTURE WORK

As a complement to probability and classical models, fuzzy logic models can be applied to assess risks for which there is high number of input factors. Fuzzy logic provides a framework where human reasoning can contribute to risk analysis and assessment. Using an appropriate fuzzy logic inference system, it is possible to consistently analyse multiple operational risks that are not well understood. The exposure to each operational risk can be assessed and evaluated. The contribution of this study is in two fold; firstly, a fuzzy logic-based OR analysis metrics was designed which includes both quantitative and qualitative parameters; which is able to work with uncertainty, imprecision and subjectivity in the data and in the analysis process. Secondly, a new factor "approximate cost of UOS" was identified to determine the magnitude of the risk impact and exposure level. Thirdly, the proposed OR analysis process consists of six factors: frequency of triggering events, effectiveness of the avoidance barriers, effectiveness of the recovery barriers, frequency of UOS occurrence, approximate cost of UOS, and severity of the (most

probable) risk impact. A combination of RCSA approach and a threat-oriented metrics approach were used. Trapezoidal fuzzy numbers were presented for computing the joint probability function of the risk factors in the OR analysis measurement.

Future work will delve into the implementation procedure of the defined measurement metrics for the analysis of E-banking operational risk using primary data reported based on surveys conducted with bank officers and the result from the implementation and evaluation will be provided. Experts with in-depth knowledge in E-banking OR can provide a valuable opinion on uncertainties. However, the quantification of their valuable knowledge to estimate the uncertainties is not an easy task. We will evaluate the model using Fuzzy Inference System that allows classification overlaps and no sharply defined boundaries because of the generalization of a characteristic function to a membership function.

REFERENCES

[1] Ako, R.E. & Okpako, A.E. (2019) A Fuzzy Logic-Based Framework for E-banking Operational Risk Assessment. *Journal of Digital Innovations & Contemporary Research in Science, Engineering & Technology,* 7(1), pp.59-74.

[2] Alam, A. Y. (2016) Steps in the Process of Risk Management in Healthcare. *Journal of Epidemiology and Preventive Medicine.* 2(2), pp. 1-5.

[3] Alkhattabi, M. A. (2010) Information Quality Assessment in E-learning Systems. *PhD thesis, University of Bradford.*

[4] Álvarez, G. & Gledhill, P. (2010) A Comprehensive Risk and Control Self-Assessment.

[5] Methodology: How to take Control, Operational Risk and Regulation, [online] London: Incisive Media, Available from: http://www.risk.net/protected/digital_assets/2281/RCSAs_OR_1210.pdf [Accessed: 26th July 2012].

[6] Álvarez, G. & Gledhill, P. (2011a) *A Comprehensive Risk and Control Self-Assessment Methodology -Part II: An RCSA Metric, Operational Risk and Regulation,* [online] London: Incisive Media, Available from: http://www.risk.net/protected/digital_assets/2433/RCSAII_OR_0111.pdf Accessed: 26th July 2012].

[7] Álvarez, G. & Gledhill, P. (2011b) *A Comprehensive Risk and Control Self-Assessment Methodology Part III: An Exercise in Self-Control, Operational Risk and Regulation,* [online] London: Incisive Media, Available from: http://www.risk.net/protected/digital_assets/2550/RCSA-III_OR_0211.pdf [Accessed: 26th July 2012].

[8] ARMS Working Group (2010) *The ARMS Methodology for Operational Risk Assessment in Aviation Organisations* [online]. Available from: http://www.skybrary.aero/bookshelf/books/1141.pdf [Accessed: 15th February 2011].

[9] Basel Committee on Banking Supervision (2011) *Principles for the Sound Management of -Operational Risk – final document*. [online]. Switzerland: Bank for International Settlements. Available from: http://www.bis.org/publ/bcbs195.pdf [Accessed: 20th January 2012]

[10] Basel Committee on Banking Supervision (2014) Review of Principles for the Sound Management of Operational Risk. [online]. Switzerland: Bank for International Settlements. Available from:https://www.bis.org/publ/bcbs292.pdf [Accessed: 27th March 2018]

[11] British Standards Institution (2010) *BS EN 31010. Risk Management – Risk Assessment Techniques.* Geneva: International Organization of Standardization.

[12] Caralli, R. A., Stevens, J. F., Young, L. R. & Wilson, W. R. (2007) *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*. Software Engineering Institute Technical Report: CMU/SEI-2007-TR-012, ESC-TR-2007-012.

[13] CRMS Indonesia, 2017, "RCSA (Risk Control Self Assessment)", [online]. http://www2.crmsindonesia.org/programs/rcsa-risk-control-selfassessment, [Accessed: 25th February 2019]13:01

[14] Guo, L. (2015) Implementation of a risk management plan in a hospital operating room. *International Journal of Nursing Sciences,* 2, pp. 348-354.

[15] International Organization for Standardization (2005) *ISO / IEC 27001. Information Technology – Security Techniques – Information Security Management Systems – Requirements.* Geneva: International Organization for Standardization.

[16] International Organization for Standardization (2009) *ISO / IEC 31000. Risk management — Principles and guidelines.* Geneva: International Organization for Standardization.

[17] International Organization for Standardization (2011) *ISO / IEC 27005. Information Technology – Security Techniques – Information Security Risk Management.* Geneva: International Organization for Standardization.

[18] Khan, M. A., Zaman S., Malik, L.F., Shah, S.J., & Waqas, A. (2014) "Implementation of Operational Risk Management Framework", State Bank of Pakistan

[19] Matthews H., & Technical Information Service (2008) Operational risk Topic Gateway Series No. 51.

[20] Martias, Andi, (2016) "Analisa Penerapan Control Self Assessment Sebagai Aplikasi Pengendalian Intern Pada PT. ABC Insurance". *Moneter*, 3(1), pp. 1-13.

[21] National Institute of Standards and Technology (2011a) *Special Publication 800-39. Managing Information Security Risk: Organization, Mission, and Information System Overview: Information Security:* Gaithersburg: Computer Security Division Information Technology Laboratory.

[22] National Institute of Standards and Technology (2011b) *Special Publication 800-30. Guide for Conducting Risk Assessments: Information Security: Revision 1: Initial Publication Draft.* Gaithersburg: Computer Security Division Information Technology Laboratory.

[23] Prospero Consulting & Training, 2018, "Perancangan Perangkat Kerja Risiko Operasional RCSA – Risk Control Self Assessment", Jakarta, Indonesia

[24] Ricci, P. F., Sagen, L. A., & Whipple, C. G. (1981) Technological Risk Assessment. *NATO Advanced Study Institute on Technological Risk Assessment – NATO ASI Series no* 81, *Conference Proceedings, Ricci P.F,* Italy, 20-31 May 1981, Netherlands, Martinus Nijhoff Publishers, pp.1-365.

[25] Setiawan, A., & Yulianto, E. (2019) Implementation Of Risk Control Self Assessments Using Rapid Application Development Model In Bank Operational Risk Management Process. *Journal of Theoretical and Applied Information Technology.* 97(11), pp. 2957-2968.

[26] Zadeh, L. A. (1965) Fuzzy sets, *Information and Control,* 8, 338-353.