Digital Innovations
& Contemporary Research in SCIENCE,
ENGINEERING & TECHNOLOGY

Vol. 7. No. 1, March 2019

Article Citation Format
Ako, R.E & Okpako, A.E. (2019): A Fuzzy Logic-Based Framework
for E-banking Operational Risk Assessment
Journal of Digital Innovations & Contemp Res. In Sc., Eng &
Tech. Vol. 7, No. 1. Pp 59-74

Article Progress Time Stamps

Article Type: Research Article
Manuscript Received: 7th Feb. 2019
Review Type: Blind
Final Acceptance:: 28th March, 2019
Article DOI: dx.doi.org/10.22624/AIMS/DIGITAL/V7N1P6

A Fuzzy Logic-Based Framework for E-banking Operational Risk Assessment

Ako, Rita Erhovwo & Okpako, Abugor Ejaita
Department of Mathematical Sciences
Edwin Clark University, Kiagbodo , Nigeria
Edwin Clark University
Kiagbodo, Nigeria
Email: ochukorita2@gmail.com; okpako.ejaita@gmail.com

ABSTRACT

Emerging realities in assessing operational risk (OR) specifically in the context of E-banking which is poised with heightened technical complexities, has raised the need for a paradigm shift from risk models based on probability and classical set theory to Fuzzy Logic (FL). Threat(s) /threat sources continue to defy probability analysis, due to uncertainties of categorizing the risks in any well-established patterns. These uncertainties which comes in different shapes and flavours such as infrequent but very large financial losses, ever changing nature of internal controls, lack of long historical data, entangled cause-and-effect relationship etc. makes it difficult to assess the exact degree of exposures to OR. Therefore it is essential to develop valid and reliable framework for effective OR assessment. Fuzzy Logic (FL) models are built upon fuzzy logic and fuzzy set theory which is suitable for analysing risks with uncertainties, incomplete data and expert opinions. In this paper, a new Operational Risk Assessment (ORA) framework for E-banking was developed using Fuzzy Logic. In addition, a new ORA factor was identified to determine the magnitude of impact and the risk exposure level.

Keywords: Fuzzy logic, operational risk, E-banking & bow-tie analysis

1. INTRODUCTION

Operational risk assessment is carried out to identify operational risk profiles, their causal relationships and measure the risk exposure levels based on the severity of occurrences, or to measure and allocate sufficient amount of risk based capital for the Value at Risk (VaR) (Teker, 2005; Basel Committee on Banking Supervision, 2011). The effectiveness of operational risk assessment is fundamental to any bank's risk management programme, as operational risk is inherent in all banking products, activities, processes and systems (Basel Committee on Banking Supervision, 2011).

In 2006, the Basel Committee on Banking developed the Basel II accord to improve the measurement of both credit and operational risks (Basel Committee on Banking Supervision, 2006), while in 2009, the Committee enhanced the measurement of risks related to securitization and trading book exposures (Basel Committee on Banking Supervision, 2009), there after developed Basel III in 2011, to strengthen the global capital requirements on bank liquidity and leverage, with the aim of raising both the quality and quantity of the regulatory capital base and enhancing the risk coverage of the capital framework (Basel Committee on Banking Supervision, 2011). Consistent with the continued focus on monitoring the implementation of its standards and guidance and in light of the significant number of recent operational risk-related losses incurred by banks, the Committee reviewed its “principles for a sound management of operational risk” guidance issued in June 2011 (Basel Committee on Banking Supervision, 2014). Four principles: change management, operational risk appetite and tolerance, disclosure, and operational risk identification and assessment, were identified as the least principle thoroughly implemented by banks (Basel Committee on Banking Supervision, 2014).

The Committee noted that failure to fully implement appropriate operational risk identification and management practices may result in direct and material financial losses, or reputational and consequential losses, and could lead to a systemic impact on other banks, customers, counterparties and the financial system (Basel Committee on Banking Supervision, 2014). As a result, the committee recommended that banks should improve the implementation of each of the operational risk identification and assessment tools, including risk and control self-assessments, key risk indicators, external loss data, business process mapping, comparative analysis, and the monitoring of action plans generated from various operational risk management tools (Basel Committee on Banking Supervision, 2014).

Further, the Payment Card Industry - Data Security Standard (PCI-DSS) council, requires all organizations involved in payment card processing – including banks, which store, process or transmit cardholder data, to annually conduct formal risk assessment in order to identify threats and vulnerabilities (PCI-DSS, 2010). The council further emphasized the need to conduct formal risk assessment by developing risk assessment guidelines version 1 & 2 in November 2012 (PCI-DSS, 2012a and 2012b) and in 2016 provided a roadmap of compliance activities based on risk associated with storing, processing, and/or transmitting cardholder data (PCI-DSS, 2016).

In addition, E-banking has undoubtedly increased the technical complexity of assessing and managing operational and security risks (Imala, 2002; Basel Committee on Banking Supervision, 2003; Bank of the Netherlands Antilles, 2007; Trenca et al, 2010), due to the intensive development of Internet technology and the evolution in telecommunication systems which provides direct, easy, anytime and anywhere access to customers in their homes, offices, and public access points. The mode of risk occurrences, magnitude, and consequences takes on new dimension (Monetary Authority of Singapore, 2002, 2008). Therefore influencing and heightening the complexity of banking institutions’ activities (Basel Committee on Banking Supervision, 2003) and the degree of uncertainty in the E-banking data (British Standards Institution, 2010). A pertinent question would be “how to effectively define a risk assessment framework for E-banking operational risk assessment that would better help the banking industries develop an effective risk management strategy”. Over the past decades, several frameworks, methodologies, tools and techniques have been developed for operational risk assessment in general. Many of these risk assessment methodologies and frameworks use the classical risk formula i.e. severity x likelihood to create a two dimensional matrix that guides the risk tolerability judgment.

Meanwhile, the development of models and frameworks for conducting E-banking operational risk assessment is relatively new, very dynamic and heterogeneous due to several security challenges such as information systems malfunctions, denial of service (DoS), identity theft, financial losses, viruses, and phishing attacks among others. New adopters lack of adequate quantitative information on the probability of risk occurrences and subjectivity involved in determining the severity of impact when a risk is released (Monetary Authority of Singapore, 2002, 2008) influences and heightens the complexity of conducting effective risk analysis. It has not been realistic to expect fully automatic, computer-based operational risk assessment systems. However, recent advances in the field of soft computing are materializing into a wider usage, armed with Artificial Intelligence (AI) techniques. Fuzzy logic techniques are computer-based system that supports reasoning under conditions of uncertainty and vagueness, and are capable of modelling cause-effect relationships at multiple levels. They are also capable of predicting future occurrences and possible intervention, which makes them attractive for E-banking operational risk assessment.

This paper focuses on the application of fuzzy logic and fuzzy set theory, introduced by mathematician Lotfi A. Zadeh in 1965, and Bow-tie analysis to E-banking operational risk assessment. In this paper, fuzzy logic was used in simulating the 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 both avoid and recover before the operational risk outcome, the estimated cost of UOS and the Severity of operational risk outcome. Moreover, the ORA framework was developed as a product of six factors indicated in a Bow-tie analysis approach and shown in a Cartesian product. The remainder of this paper is organized as follows: Section 2 gives a literature review. Section 3 discusses the existing ORA frameworks. Section 4 presents the proposed ORA framework. Conclusion and future work are given in section 5.

2. LITERATURE REVIEW

Aburrous et al. (2008), proposed a model for assessing and evaluating E-banking security website (i.e. an asset driven risk) based on fuzzy logic approach. The model consists of four stages: fuzzification of input variables, rule evaluation, aggregation of the rule outputs, and defuzzification. Their model addresses E-banking website by classifying all Internet banking risks, threats, and vulnerabilities according to an important weight. The goal is to identify the risk with large impact on the E-banking website security and performance. They assessed the website security using four main risk attack criteria: direct internal attack, communication tampering attack, code programming attack and denial of service attack. These four criteria are classified into a hierarchical ring layer structure and prioritized according to their importance using the weights concluded from their bank IT auditors' survey.

Tanampasidis (2008), proposed a methodology for assessing E-banking operational risk, which uses a Key Risk Indicator (KRI), self-assessment and expert opinion approach. The overall goal is to identify the level of risk exposures, the residual risk for further investigation, assess areas where risk is eliminated or insignificant, and the areas where risk is relatively high or sensitive. The assessment process is carried out based on six major steps and includes Strategy analysis and evaluation, risk identification, identification of points of risk mitigation and control, risk evaluation, risk measurement, and reports. This E-banking operational risk assessment process requires an external auditor to identify key risk areas, while the business users assess the level of risk exposure for each area / risk factor. Reliability of the results depends on the degree to which both the risk analyst and business users actively participate in the assessment process.

In addition, different analysts may provide different set of Key Risk Factors (KRFs), thus results are not comparable to other similar surveys or even previous surveys in the same organization. It is pertinent to note that KRIs cannot take into account process changes and system upgrades. Nevertheless, it has been shown that auditors with average experience will provide similar sets of KRFs.

ISACA (2009), developed an IT Risk framework to enable organizations integrate IT risk management into their overall Enterprise Risk Management (ERM). The IT Risk framework addresses risk governance, risk evaluation, and risk response. Each of these domains is assigned a process detail, goals and metrics. The goal of the framework is to help organizations make well-informed decisions about the extent of their risk, risk appetite and risk tolerance, and to understand how to respond to the risk. In the context of risk evaluation (i.e. risk assessment) the typical aspect of their framework includes data collection, risk analysis and risk profile management. They opined that Risk IT framework fills the gap between generic risk management frameworks, standards and principles such as COSO7, AS / NZS 4360, ISO 31000, the UK – based risk management standard and domain specific frameworks.

ARMS Working Group Methodology and Framework (ARMS Working Group, 2010), proposed an operational risk assessment methodology and framework for flight safety risk assessment. They developed the safety risk assessment framework based on four factors: frequency of triggering event, effectiveness of avoidance barriers, effectiveness of recovery barriers, and severity of the most probable accident outcome. These four factors form the major part of their risk assessment framework known as the Safety Issue Risk Assessment (SIRA) framework. The framework expand upon the classical risk assessment formula (severity x likelihood) and together determines the risk exposure level. The SIRA Framework is a process which requires first a clear definition and scope of the safety issue and to quantify the assessment using a formula where risk has the four factors. The values for these factors can be qualitative classes or numerical where the first three factors define the mean frequency of the accident, while the fourth factor defines the most probable severity of the outcome. The resulting output of the SIRA process is a risk value for each safety issue.

Montewka et al. (2014), proposed a risk assessment framework for estimating the risk of maritime transportation. They applied Bayesian Belief Networks as the tools for knowledge representation and efficient two-way reasoning under uncertainty. They addressed the uncertainties inherent to model variables by describing variables using distributions obtained in the course of numerical analysis. Epistemic uncertainties related to model structure are analysed by performing alternative hypotheses testing. They developed a set of scenarios with constant set of variables with different plausible hypothesis guiding the links between variables. The resulting output of the framework is communicated in the form of a diagram, representing the cumulative distribution of likelihood of the occurrence of number of fatalities given the scenarios.

One significant work towards risk assessment framework has been presented by Toth-Laufer et al. (2015), where fuzzy logic-based decision making in a hierarchical, clustered structure was used to evaluate physiological parameters of patient. The risk assessment framework is applied in sport activity by calculating the risk level based on physiological and other personal parameters specific to the user to control the patient continuously. They formed three subsystems based on the clusters which belong to different risk groups (medical condition, activity load and environmental conditions). The three groups are then used to determine the risk level of physical activity and finally the total risk level. The resulting output is the evaluation of the individual characteristics, living conditions, habits and medical recommendations.

These are based on the personal profile, in which different parameter combinations can be defined for each user and can be modified and broadened specifically to the user.

2.1 Bow Tie Analysis

The British Standards Institution (BSI) (2010), defined Bow-tie analysis as a simple diagrammatic framework for integrating and analysing the pathways of a risk from cause to consequences. It is used for displaying a risk showing a range of triggering events and consequences of risk outcome, while taking into consideration the controls or barriers put in place (BSI, 2010; ARMS Working Group, 2010). The focus of Bow-tie analysis is on the preventive barriers, which lie between the causes and the risk, and the recovery barriers, which lie between the risk and the risk consequences.

Although, Bow-tie analysis has proven valuable for describing risk assessment process, it may oversimplify complex problems where quantification is attempted. It is also not capable of revealing in the diagram where multiple causes occur simultaneously to cause the consequences, and therefore an earlier risk identification process is required. The quality of the analysis will also depend solely on the quality of the analysis process, and the analysts or domain experts. In addition, analysis may be influenced by staff members or experts with a differing agenda to that of the organization, as a result additional supporting information may be required either from external data or other relevant documents (McConnell & Davies, 2006; BSI, 2010; ARMS Working Group 2010; Mokhtari et al., 2011). Figure 1 below represents a general Bow-tie diagram. In recent times, the focus on products and services has shifted largely to a focus on customers (Vargo and Lusch, 2006).

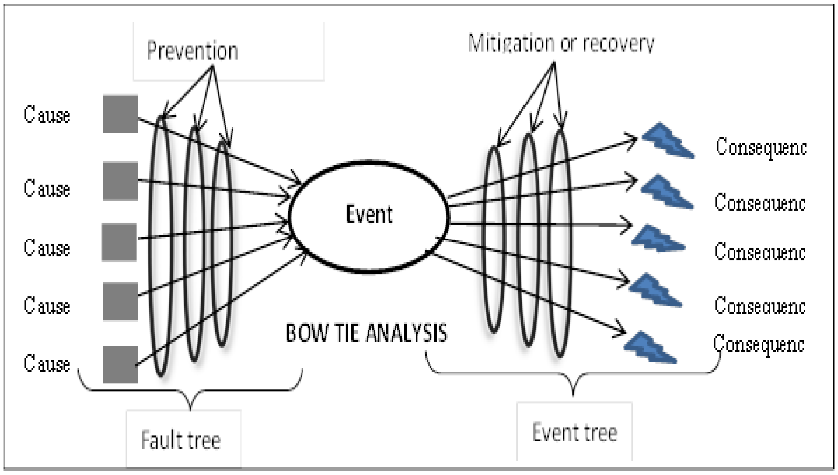


Fig 1: A General Bow-Tie Analysis

A number of research groups have proposed Bow-tie analysis to managing and developing risk assessment; to mention a few: McConnell & Davies (2006), ARMS Working Group (2010) and Mokhtari et al (2011). McConnell & Davies (2006) proposed Bow-tie analysis for conducting safety operational risk management in the scenario analysis under the Advanced Management Approach (AMA) required by the Basel II accord. Similar to McConnell & Davies, the ARMS Working Group (2010) proposed Bow-tie analysis technique to aircraft safety issues identification and computation by quantifying the five factors identified within the Bow-tie sequence.

Mokhtari et al (2011) on the other hand proposed Bow-tie analysis to managing sea ports and offshore terminal risk.

3. Analysis of Existing Risk Assessment Frameworks

Proper identification and assessment of risk is the major concern in risk management, it is therefore imperative to have systems that assist risk professionals with such an accuracy and classification efficiency to human reasoning under uncertainty. Many existing systems have employed different approaches in ameliorating the effect of risk uncertainties yet there is still room for improvement so as to handle risk exposure level classification. A detailed review and analysis of existing systems 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 assessment process and specifically E-banking systems. Two frameworks were considered here, they are the SIRA framework by (ARMS working group, 2010) and the ISACA IT framework by (ISACA, 2009).

We reviewed the following:

i. The approaches and methods used in the existing risk assessment framework,
ii. The factors and inference mechanism for determining the risk exposure levels,
iii. The decision support tools for identifying and evaluating the risk analysis process.

The ARMS framework employs the principles of the BS ISO / IEC 31010:2010 and BS / ISO 31000:2009 standards. This framework referred to as SIRA tool was developed using Excel-based application. In the SIRA framework, the adequacy of planned or existing security controls were taken into account and included at the level of risk determination. Figure A.1 shows the ARMS SIRA framework. The resulting output of the SIRA process is a risk value for each safety issue. The output result was produced using JAR/FAR-1309 limits on a scale of five levels of risk.

Unacceptable levels of risk:

- Stop
- Improve

Tolerable levels of risk:

- Secure
- Monitor
- Accept

However, the SIRA method works when there are enough factual, quantifiable elements to feed the SIRA. Therefore for purely qualitative “soft” changes it may be impossible to quantify the risk using ARMS and hence the SIRA framework cannot be used. Thus the emerging reality is the use of qualitative assessment that is based on domain expert judgments. In addition, the ARMS Working Group framework failed to identify the importance of including in the risk assessment, the cost for UOS or the assets value (see ISO / IEC 27005:2011). Apart from identifying the ARMS Working Group safety issue framework, the ISACA Risk IT framework was also identified. The typical aspect of their framework is the development of four risk analysis stages: defining the IT risks analysis scope, estimating IT risk, Identifying risk response options and performing a peer review of IT risk analysis. The resulting output of the risk analysis stage is the risk analysis scope, the scenario analysis results, the risk analysis results and the peer-review recommendations.

Interestingly, in the two frameworks reviewed it was found that there was no general consensus on used risk assessment factors. Two common risk assessment attributes (frequency of occurrence and severity of impact estimation) were used. However our focus is on the SIRA framework by the ARMS working group, (2010). The SIRA framework has the ability of significantly shifting from classical risk assessment methods to a new risk assessment method which addresses the problems of the modern electronic era.

4. DESIGN OF THE PROPOSED ORA FRAMEWORK

Several researchers have applied different approaches to assessing risks and from the analysis of our considered existing system, several limitations or drawbacks were observed and highlighted for our proposed framework to tackle. In this work, the ORA framework includes the following stages: (1) Risk issue identification, (2) development of the related potential risk scenarios, (3) analysis of potential risk scenario, (4) description of barriers and cost estimation, (5) risk assessment and (6) risk exposure level and evaluation determination.

1. Identify clearly the various Risk Issues in the E-banking system under study
   - Based on literature, dataset/databases analysis results using a TAN model (Ako & Okpako, 2018).
2. Define the risk issues/factors precisely.
   - Scope the selected issue in terms of identified risks, scenario description, locations, E-banking types or processes, and time-period under study.
3. Develop the related potential risk scenarios using Bow tie analysis.
   - There may be several risk scenarios within one risk / risk factors.
   - Select the most critical scenarios (one or more) for the risk assessment, alternatively aggregate them if possible.
4. Analyse each potential risk scenario using the ORA framework.
   - Identify what is considered the triggering event
   - List the avoidance barrier (controls) and review its robustness
   - Decide what is considered the Undesirable Operational State (UOS)
   - List the recovery barriers (controls) and review their robustness
   - Define the risk outcome of the scenario
   - Determine the estimated cost for UOS occurrence
5. Run the ORA with values
   - Using FL approach for each risk attribute rating.
   - Apply FIS or other matrix formulation tools.
   - Select a known or an estimated value for each of the six ORA component.
   - Use a scale of three, five or more parameters
6. Determine the risk exposure level using a scale of three, five or more risk classes
   - Classify the resulting risk class and security level.
   - Make recommendations.
   - Generate reports.

In the considered existing framework four factors were identified and were used as a fundamental base to which new factors was discovered for E-banking OR assessment. In addition, Bow tie analysis technique and Fuzzy logic model was employed to the six identified risk factors in order to assess the degree of risk exposure and their resulting risk class, considering both the available data and experts' opinions, which will ultimately be used to determine the security posture of the E-banking system.

Our proposed framework shown in figure A.2 and A.3 exhibit three major characteristics or uniqueness:

i. An approximate cost for the UOS: It was noticeable that including "approximate cost for UOS" would help in identifying more clearly the magnitude of impact and the risk exposure level as against the approximate cost for each occurrence of the threat-source's exercising the vulnerabilities, suggested in the NIST SP 800-30:2011 methodology. Considering the approximate cost for each occurrence of the threat-source's exercising the vulnerabilities is rather vague and highly subjective, because the number of vulnerabilities tends to be large, as a result identifying the cost is complex and most likely impractical.

ii. The Bow tie analysis technique: it has been extended for developing the E-banking OR assessment framework because it takes into account not just the frequency × severity formula for risk occurrences but also the barriers in place to both prevent and recover from UOS occurrences, starting from the complex linkages between triggering events and the potential risks outcome.

iii. Fuzzy logic models: they are built upon fuzzy set theory and fuzzy logic. In contrast classical risk models are based on probability and classical set theory. The fundamental difference between classical set theory and fuzzy set theory is the inclusion of elements in the set. In traditional sets, an element is either included in the set or is not. In a fuzzy set, an element is included with a degree of membership ranging from 0 to 1. Fuzzy logic models allow an object to be categorized in more than one exclusive set with different levels of truth or confidence. They are useful for analysing risks with incomplete knowledge or imprecise data and consider explicitly the cause –and–effect relationship among risk variables that are described in linguistic terms. Risk analysts may not have enough knowledge or sufficient data for a comprehensive risk assessment using models based on probability theory.

The inference mechanism of using the notion of fuzzy logic- representing truth membership function such as the likelihood of some event or condition rather than using the classical risk formula of severity x likelihood for the risk exposure level determination makes fuzzy logic models more intuitively similar to human reasoning. Fuzzy logic models provides a framework in which experts' input and historical data can be used to jointly assess the uncertainty, identify major risk issues and assess exposure to these risks. In addition, fuzzy logic models include rules that explicitly explain the linkage, dependence and relationships among modelled factors. It is helpful for identifying risk mitigation decisions. Resources can then be used to mitigate the risks with the highest level of exposure.

4.1 Underlying Concepts of the Proposed Framework

This section discusses the underlying concepts that make up the proposed framework.

Bow Tie Analysis

The operational risks are displayed in the bow tie analysis by showing a range of triggering risk events and consequences of the risk outcome, while taking into consideration the controls or barriers put in place. In constructing the Bow tie diagram, a clear understanding of the information based on the Bow tie sequence is required by the modellers or risk analysts. Each of these paths or stages are analysed by the experts and brought together into a coherent whole. The Bow tie sequence in the system understudy is expressed as: Triggering events → Barriers to avoid UOS → UOS → Barriers to recover before risk outcome → Risk outcome. Fault tree analysis (FTA) which is the left-hand side of the diagram can be used to analysing the cause of an event, while Event tree analysis (ETA) which is the right-hand side of the diagram can be used to analysing the consequences as shown in figure 1. Thus the Bow tie diagram may start from the FTA to the ETA. However, Bow tie diagrams are mainly used when the problem or situation does not require the complexity of a full fault tree analysis or when the focus is to ensure barriers or controls for each path in the

Bow tie diagram are in place. As a result it is often drawn directly from a brainstorming session.

Fuzzy Logic and Fuzzy Set Theory

Lotfi A. Zadeh in the mid-1960s developed fuzzy logic and fuzzy set theory to model those problems in which imprecise data must be used or in which the rules of inference are formulated in a very general way making use of diffuse categories (Rojas, 1996). Zadeh, defined fuzzy set as a class of objects with a continuum of grades of membership. Such fuzzy set is characterized by a membership function which assigns to each object a grade of membership ranging between 0 (completely false) and 1 (completely true). Fuzzy set theory allows an object belong to multiple exclusive sets in the reasoning framework. For each set, there is a degree of truth that an object belongs to a fuzzy set. In fuzzy set theory, fuzzy set A of universe X is defined by function $\mu_A(x)$ called the membership function of set A

This is best captured in equation 1.

$$\mu_A(x): X \to [0,1], \qquad \text{Eq. (1)}$$

where

$\mu_A(x) = 1$ if x is totally in A;

$\mu_A(x) = 0$ if x is not in A;

$0 < \mu_A(x) < 1$ if x is partly in A.

This set allows a continuum of possible choices. For any element x of universe X, membership function $\mu_A(x)$ equals the degree to which x is an element of set A. This degree is a value between 0 and 1, which represents the degree of membership, called membership value of element x in set A. In this framework, Fuzzy logic is used to evaluate the risk exposure level based on six identified OR factors: Triggering Events (TE), Avoidance Barriers (AB), Recovery Barriers (RB), Undesirable Operational State (UOS) occurrence, Cost of UOS, and Severity of Risk Outcome (SRO) and as shown in Figure A.2 and A.3 below. The formula for the ORA is calculated as a product of the six factors indicated in the Bow-tie analysis structure and as shown in the Cartesian product:

$$Risk\ Exposure\ Level\,(REL) = \\ TE \times AB \times UOS \times Cost\ of\ UOS \times RB \times SRO \qquad \text{Eq. (2)}$$

The fuzzy logic framework uses linguistic variables and descriptors to represent the OR factors which are assigned to a range of values. The input and output linguistic variables, as well as their ranges are predefined by the analyst from a combination of dataset/database and experience. Having specified the risks assessment factors and parameters (param_1 to param_n) of the membership functions, the next step is to specify how the E-banking OR probability varies. All of the risk factors and risk levels can be quantitative or given in linguistic form. Experts often provide fuzzy rules in the form of if…then statements that relate E-banking OR probability to various key risk indicators / factors based on their knowledge and experience. The proper operation of the system greatly depends on the applied rule base, which should be risk issue-specific as far as possible. The evaluation of the risk factors and the determination of the risk exposure level is obtained by an approximate fuzzy inference system (FIS) (e.g. Mamdani FIS, Mamdani-like structure with discretized output).

The level of risk associated with identified risk represents a determination of the degree to which organizations are threatened by such risk.

Approximate Cost of UOS

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. The approximate cost of UOS 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. For example an attacker (insider or outsider fraudster) pretended to be a legitimate M-banking agent because he / she was able to gain unauthorized access to the M-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.

5. 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, which includes both quantitative and qualitative parameters; which is able to work with uncertainty, imprecision and subjectivity in the data and in the assessment process. Fuzzy logic provides a framework where human reasoning can contribute to risk analysis and assessment. Key operational issues risks can be identified and exposure levels can be assessed and evaluated. Fuzzy logic models may be used with other risk models such as bow tie analysis to model complex operational risk issues in E-banking systems. The key quality in this study is to achieve a better and proper assessment process of E-banking operational risk profiles. The contribution of this study is in three fold; firstly, a fuzzy logic-based ORA framework was designed, while the adaptive capacity of the system is improved. Secondly, a new factor "approximate cost of UOS" was identified to determine the magnitude of impact and the risk exposure level. Thirdly, the proposed ORA framework 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 indicated in the Bow tie analysis. The ARMS Working Group framework was adopted and used as a guide; as it employs the principles of the BS ISO / IEC 31010:2010 and BS / ISO 31000:2009 standards.

Future work will delve into the implementation procedure of the framework for the assessment of E-banking operational risk using both primary and secondary data analysis and the result from the implementation and evaluation will be provided.

REFERENCES

[1] Aburrous, M, Hossain, M. A., Dahal, K., & Thabtah, F. (2010) Intelligent Phishing Detection System for E-banking using Fuzzy Data Mining. Journal of Expert Systems with Applications, 37(12), Las Vegas, NV, IEEE, pp.7913-7921.

[2] Ako, R. E. & Okpako, A. E. (2018) A Causality Learning of E-banking Operational Risk using Tree Augmented Naïve Bayes Classifier. International Journal of Soft Computing and Engineering, 8(4), pp. 22-37.

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

[4] 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].

[5] 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].

[6] 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]

[7] Bank of the Netherlands Antilles (2007) Provisions and Guidelines for Safe and Sound Electronic Banking, December 2007 Available: http://www.centralbank.an/uploads/files/ElectronicBanking.pdf [Accessed: 16th February 2012]

[8] Basel Committee on Banking Supervision (2003) Risk Management Principles for Electronic Banking-Final Document [online]. Switzerland: Bank for International Settlements. Available from: http://www.bis.org/publ/bcbs98.pdf [Accessed: 20th April 2007]

[9] Basel Committee on Banking Supervision (2006). International Convergence of Capital Measurement and Capital Standards: A Revised Framework Comprehensive Version [online]. Switzerland: Bank for International Settlements. Available from: http://www.bis.org/publ/bcbs128.pdf [Accessed: 6th January 2009]

[10] Basel Committee on Banking Supervision (2009). Enhancements to the Basel II Framework [online]. Switzerland: Bank for International Settlements. Available from: http://www.bis.org/publ/bcbs157.pdf [Accessed: 5th January 2012]

[11] 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]

[12] 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]

[13] British Standards Institution (2009) BS ISO 31000. Risk Management – Principles and Guidelines. Geneva: International Organization of Standardization.

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

[15] Dunham, M. (2003) Data Mining Introductory and Advanced Topics. China: Pearson Education Asia Limited and Tsinghua University Press.

[16] Imala, O. I. (2002) Electronic Commerce and Telecommunications in Nigeria: Bank Regulator Perspective, paper presented at the International Conference on Electronic Commerce and Telecommunications in Nigeria, Lagos, 23rd September.

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

[18] ISACA, (2009) The Risk IT Framework. ISBN:9781604201116.

[19] McConell, P. & Davies, M. (2006) Safety First – Scenario Analysis under Basel II [online]. Virginia, USA: Portal Publishing Ltd. Available from: http://www.continuitycentral.com/SafetyFirstscenarioanalysis.pdf [Accessed: 22nd January 2012].

[20] Mokhtari, K., Ren, J., Roberts, C., & Wang, J. (2011) Application of a Generic Bow-tie based Risk Analysis Framework on Risk Management of Sea Ports and Offshore Terminals. Journal of Hazardous Materials, 192(2), pp. 465-475.

[21] Monetary Authority of Singapore (2002). Internet Banking Technology and Risk Management Guidelines version 1.2.

[22] Monetary Authority of Singapore (2008). Internet Banking Technology and Risk Management Guidelines version 3.

[23] Montewka et. al (2014) A Framework for Risk Assessment for Maritime Transportation Systems-A Case Study for Open Sea Collisions Involving RoPax Vessels. Journal of Reliability Engineering Systems safety, 124, pp. 142-157.

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

[25] Negoita, M., Neagu, D., & Palade, V. (2005) Computational Intelligence: Engineering of Hybrid Systems. Heidelberg: Springer-Verlag.

[26] Payment Card Industry - Data Security Standard (2010) Self-Assessment Questionnaire D and Attestation of Compliance. Self-Assessment Questionnaire D version 2.0, Payment Card Industry Security Standards Council.

[27] Payment Card Industry - Data Security Standard (2012a) Information Supplement: PCI DSS Risk Assessment Guidelines version 1.0, Risk Assessment Special Interest Group and PCI Security Standards Council.

[28] Payment Card Industry - Data Security Standard (2012b) Information Supplement: PCI DSS Risk Assessment Guidelines version 2.0, Risk Assessment Special Interest Group and PCI Security Standards Council.

[29] Payment Card Industry - Data Security Standard (2016) PCI DSS Prioritized Approach for PCI DSS 3.2, PCI Security Standards Council.

[30] Rojas, R. (1996) Neural Networks – A Systematic Introduction. Springer-Verlag, Berlin, New-York 502, p.350.

[31] Shah, M., Pandya, A., Yadav, A., Chitalia, Y., & Row, D.T. (2014) A Fuzzy Logic Based Food Security Risk Level Assessment. International Journal of Emerging Technology and Advanced Engineering. Vol 4(12), pp. 547-551.

[32] Shah, S. (2003) Measuring Operational Risks using Fuzzy Logic Modelling [online]. Available from: http://www.prmia.org/Chapter_Pages/Data/WashingtonDC/Shah_Paper_1_26_05.PDF [Accessed: 6th January 2012].

[33] Tanampasidis, G. (2008). A Comprehensive Method for Assessment of Operational Risk In E-banking. International Systems Control Journal, 4, pp.1-7.

[34] Teker, D. (2005). Comparative Analysis of Operational Risk Measurement Techniques. International Conference Trade and Finance Association. 15th International Conference, Istanbul, Turkey, May 2005, The Berkeley Electronic Press, pp.1-24.

[35] Toth-Laufer, E., Takacs, M., & Rudas, I. J. (2015) Fuzzy Logic-based Risk Assessment Framework toEvaluate Physiological Parameters. Journal of Acta Polytechnica Hungarica, Vol 12(2), pp.159-178.

[36] Trenca, I., Silivestru, H., & Paun, D. (2010) New Trends Concerning Operational Risc in E-banking. Analele Stiintifice ale Universitatii "Alexandru Ioan Cuza" din Iasi, Vol 2, pp.171-180.

[37] Vargas, R. E. (2009) Fuzzy Logic: Theory, Programming, and Applications. Hauppauge, NY: Nova Science.

[38] Venugopal, K. R., Srinivasa, K.G., & Patnaik, L. M. (2009) Soft Computing for Data Mining Applications. New York: Springer.

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

[40] Zadeh, L. A. (1992) Fuzzy Logic for the Management of Uncertainty. New York: John Wiley.

[41] Zadeh, L. A. (2004). Fuzzy Logic Systems: Origin, Concepts, and Trend. Hong Kong, November 2004.

APPENDIX A

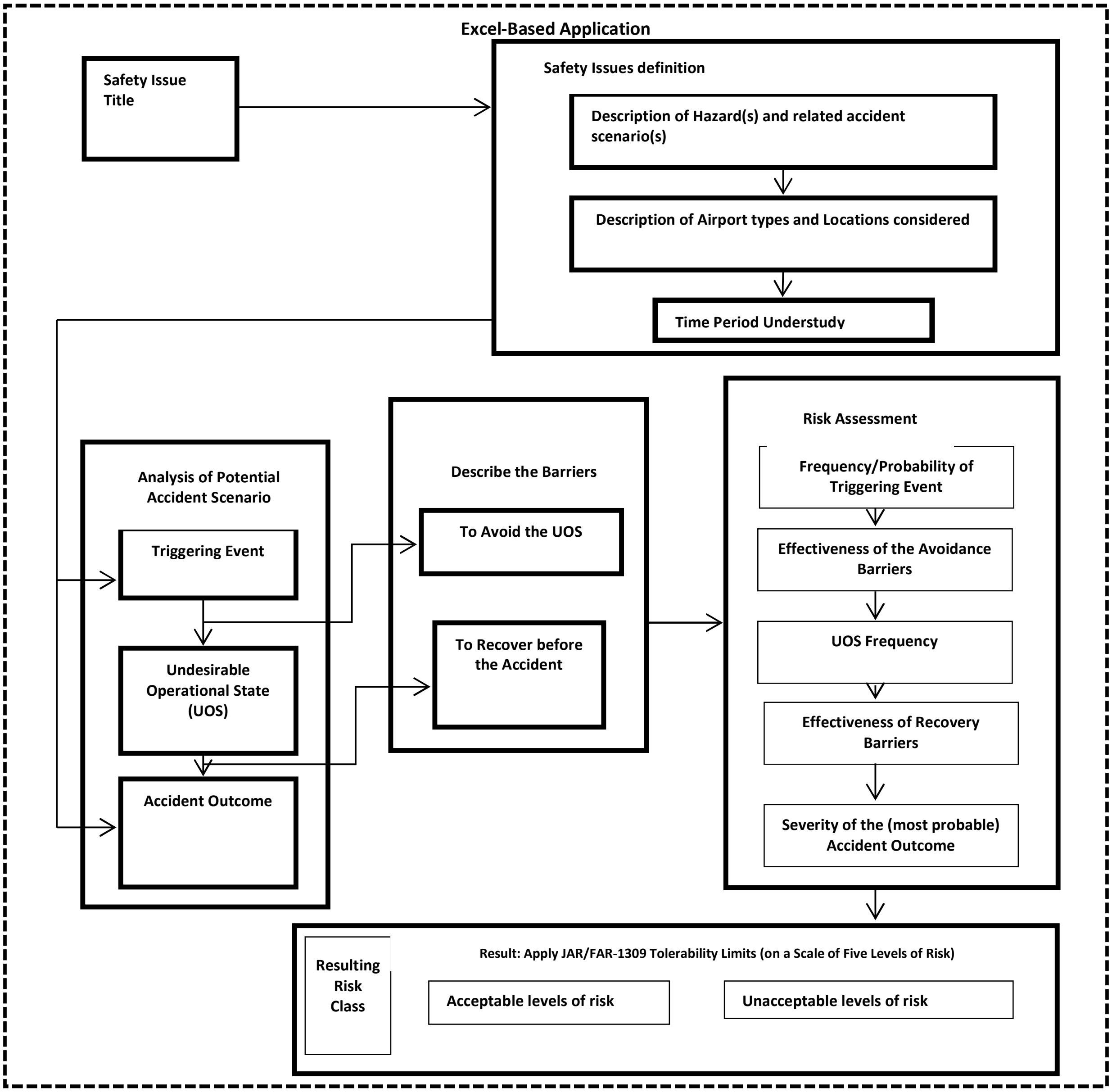

Excel-Based Application
Safety Issue Title
Safety Issues definition
Description of Hazard(s) and related accident scenario(s)
Description of Airport types and Locations considered
Time Period Understudy
Analysis of Potential Accident Scenario
Triggering Event
Undesirable Operational State (UOS)
Accident Outcome
Describe the Barriers
To Avoid the UOS
To Recover before the Accident
Risk Assessment
Frequency/Probability of Triggering Event
Effectiveness of the Avoidance Barriers
UOS Frequency
Effectiveness of Recovery Barriers
Severity of the (most probable) Accident Outcome
Resulting Risk Class
Result: Apply JAR/FAR-1309 Tolerability Limits (on a Scale of Five Levels of Risk)
Acceptable levels of risk
Unacceptable levels of risk

Figure A.1: ARMS SIRA Framework

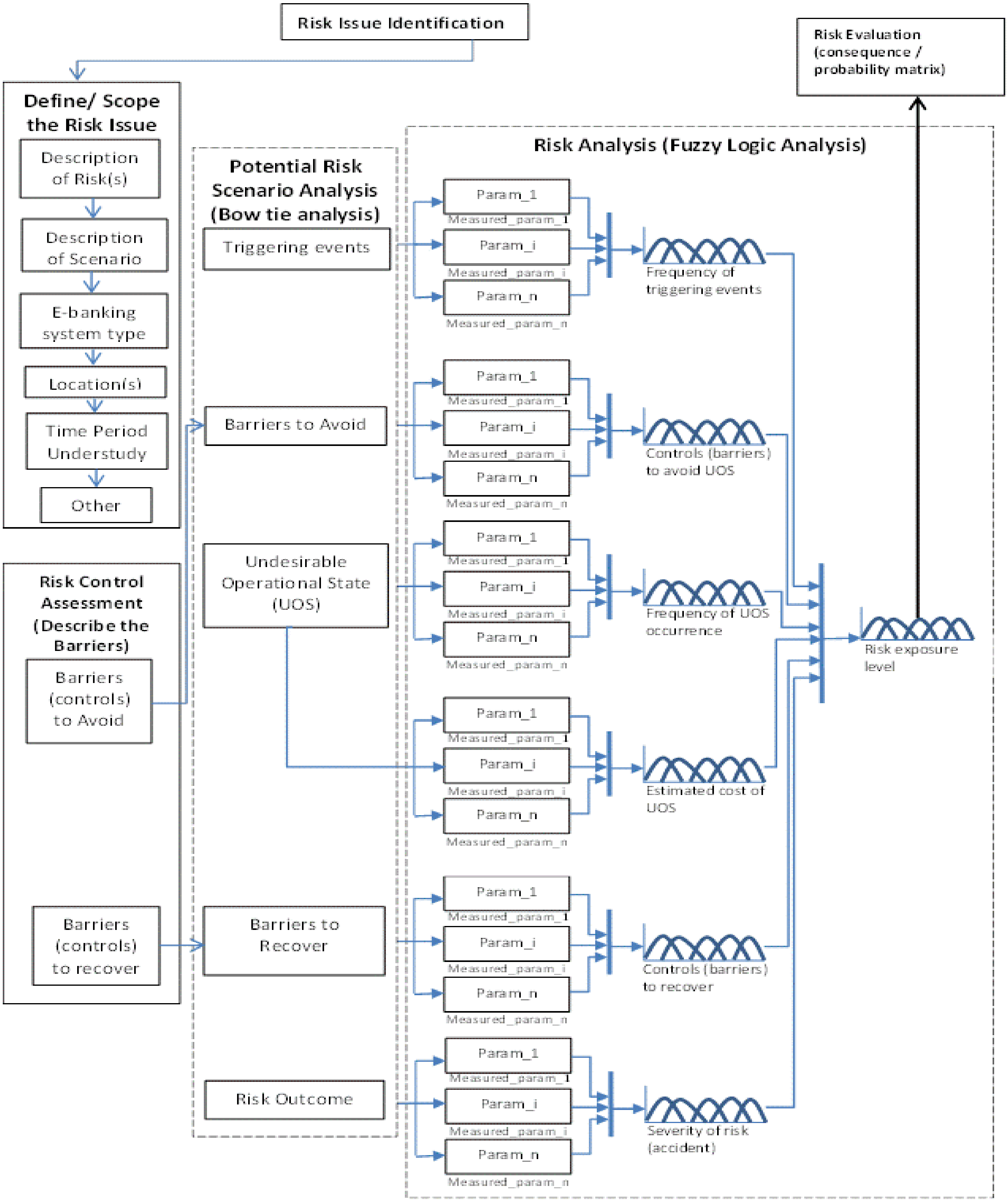
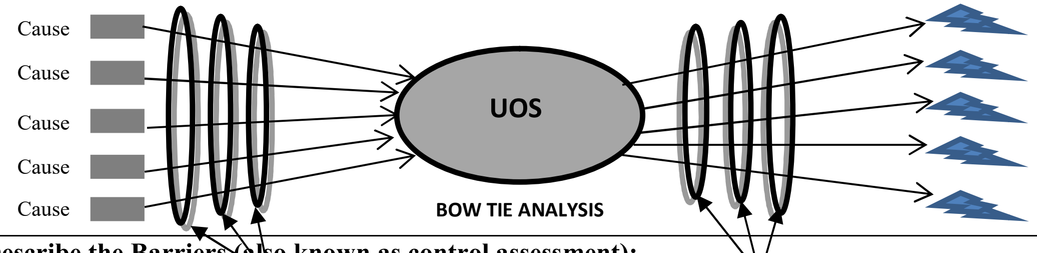

Risk Issue Identification
Define/ Scope the Risk Issue
Description of Risk(s)
Description of Scenario
E-banking system type
Location(s)
Time Period Understudy
Other
Risk Control Assessment (Describe the Barriers)
Barriers (controls) to Avoid
Barriers (controls) to recover
Potential Risk Scenario Analysis (Bow tie analysis)
Triggering events
Barriers to Avoid
Undesirable Operational State (UOS)
Barriers to Recover
Risk Outcome
Risk Analysis (Fuzzy Logic Analysis)
Param_1
Measured_param_1
Param_i
Measured_param_i
Param_n
Measured_param_n
Frequency of triggering events
Controls (barriers) to avoid UOS
Frequency of UOS occurrence
Estimated cost of UOS
Controls (barriers) to recover
Severity of risk (accident)
Risk exposure level
Risk Evaluation (consequence / probability matrix)

Figure A.2: Proposed ORA Framework

	E-BANKING OPERATIONAL RISK ASSESSMENT (ORA) FRAMEWORK	
1	**Risk Issue Identification:**	
2	**Define / Scope the Risk Issue:**	
2.1	Description of risk(s)	
2.2	Description of scenario	
2.3	E-banking system type	
2.4	Location(s)	
2.5	Time period understudy	
2.6	Other	
3	**Analysis of Potential Risk Scenario (also known as Bow tie analysis):**	

3.1Triggering events	3.2 Undesirable Operational State (UOS)	3.3 Risk (accident) outcome



4 **Describe the Barriers (also known as control assessment):**

	4.1 Barriers (existing controls) to avoid the UOS		4.2 Barriers (existing controls) to recover before the risk (accident)	

5 **Risk Analysis (also known as fuzzy logic analysis):**

5.1 The estimated frequency of triggering events (per specified users)	5.2 The barriers will fail in avoiding the UOS (per specified attacks)	5.3 The frequency of UOS occurrence (per specified attacks)	5.4 The barriers will fail in recovering the situation before the accident	5.5 The estimated cost of UOS (expert specified value range)	5.6 The severity of risk (accident) would be
❖ Very frequent ❖ Frequent ❖ Occasional ❖ Rare ❖ Very rare	❖ Practically always ❖ Often ❖ Sometimes ❖ Rarely ❖ Very rarely	❖ Very frequent ❖ Frequent ❖ Occasional ❖ Rarely ❖ Very rare	❖ Practically always ❖ Often ❖ Sometimes ❖ Rarely ❖ Very rarely	❖ Very high ❖ High ❖ Average ❖ Low ❖ Very low	❖ Extremely severe ❖ Moderately severe ❖ Somewhat severe ❖ Slightly severe ❖ Not at all severe

6 **Risk Exposure Level Classification** **Fuzzy Logic based on attribute representation**

6.1 Resulting risk class: ❖ Very high ❖ High ❖ Moderate ❖ Low ❖ Very low **Fuzzy Logic based on attribute respresentation**	**7** **Risk Evaluation (also known as consequence / probability matrix):** 7.1Security level / decision: **STOP** **IMPROVE** **SECURE** **MONITOR** **ACCEPT**
8 Documentation:	

Figure A.3: The Expanded Components of the ORA Framework