Scientia Africanica, Vol. 19 (No. 3), December, 2020. Pp 101-124 https://dx.doi.org/10.4314/sa.v19i3.8
© Faculty of Science, University of Port Harcourt, Printed in Nigeria *ISSN 1118 – 1931*

A METHODOLOGY FOR E-BANKING RISK ASSESSMENT USING FUZZY LOGIC AND BAYESIAN NETWORK

Ako Rita Erhovwo[1], Okpako Abugor Ejaita[2] and Oghorodi, Duke[3]

[1]Department of Mathematical Sciences, Edwin Clark University, Kiagbodo, Nigeria
[2] Department of Mathematical Sciences, Edwin Clark University, Kiagbodo, Nigeria
[3] Department of Computer Science, College of Education, Warri, Delta State, Nigeria.
ochukorita2@gmail.com ; okpako.ejaita@gmail.com ; dukeoghorodi@gmail.com

Received: 28-09-2020
Accepted: 13-10-2020

ABSTRACT

Risk assessment methodology in general has been around for quite a while, its prominence in the E-banking field is a fairly recent phenomenon. We are at the point where risk assessments are critical to the overall function of banks. Banks are required to assess the processes underlying their operations against potential threats, vulnerabilities, and their potential impact, which helps in revealing the risk exposure level, and the residual risks. Identifying clearly a risk assessment methodology is often the first step of assessing and evaluating risk associated with an organization operation. This paper presents a risk assessment methodology for E-banking Operational Risk. The proposed risk assessment methodology consists of four major steps: a risk model, assessment approach, analysis approach and a risk assessment process. The main tool of the proposed risk assessment methodology is the risk assessment process. The assessment process gives detailed explanation with respect to which models or techniques may be applied and how they are expressed. In this paper the risk assessment technique is built upon fuzzy logic (FL) concept and Bayesian network (BN). In fuzzy logic, an element is included with a degree of membership. Bayesian network is an inference classifier that is capable of representing conditional independencies. The Bayesian and fuzzy logic–based risk assessment process gives good predictions for risk learning and inference in the E-banking systems.

Keywords: Fuzzy logic, Bayesian network, risk assessment methodology, operational risk, E-banking

INTRODUCTION

In today's world of high reliance on complex and sophisticated technology, the major challenges for organizations is not only keeping up with security and technological changes, but also the adoption of effective risk assessment methodologies that will help to determine the risk exposure level / security posture associated with the organization's system or processes. Defining clearly the risk assessment methodology is often the first step to assessing risk associated with an organization operation. Risk assessment methodology is defined as *"a risk assessment process, together with a risk model, assessment approach, and analysis approach"* (National Institute of Standards and Technology, 2011b). Any assessment of risk must include an explicit risk model, assessment process and an analysis approach. There are a number of risk assessment methodologies which are often developed to identify risks, measure risk exposure levels and determine the residual risks (Tanampasidis, 2008).

However, within the recently published literature, it was found that there was no consensus on the risk assessment process. In general, two common risk assessment attributes (likelihood of occurrence and severity of impact estimation) were used in reviewed methodologies. Many of the risk assessment methodologies are using the classical risk formula i.e. *severity x likelihood* to create a two dimensional matrix that guides the risk tolerability judgment. These methodologies uses control effectiveness values obtained during Risk and Control Self-Assessment (RCSA) as the overall severity rating scale for a given potential vulnerability (National Institute of Standards and Technology, 2011b). The assumption is that control effectiveness value is equal to the severity level of potential vulnerabilities, which is rather vague and highly subjective. Such an approach is failing nowadays as we move towards a more dynamic environment of knowledge, dependent on human driven information society. In addition, the definition of what these attributes mean and how they are employed in the risk analysis process differs between researchers and organizations. It is therefore essential to develop valid and reliable methods for effective risk assessment and evaluations.

This paper reviewed seven risk assessment methodologies and proposed a Bayesian network and fuzzy logic based methodology for E-banking Operational Risk Assessment (ORA), which consists of four major steps: a risk model, assessment approach, analysis approach and a risk assessment process. The main tool of the proposed risk assessment methodology is the risk assessment process. The risk assessment process is based on fuzzy concept and Bayesian network which are capable and useful for analysing risks with incomplete data, uncertainty, and expert opinion. The E-banking OR assessment process gives detailed explanation with respect to which models or techniques may be applied and how they are expressed. Although, the sub-processes are sequenced, the E-banking OR assessment process is iterative and allows feedback.

LITERATURE REVIEW

In this section a detailed review and analysis of existing risk assessment methodologies was carried out in order to bring to fore areas to improve on. This process was necessary in order to identify new risk assessment processes and attributes, in order to tackle the vagueness and dynamic environment to assessing operational risk inherent in an E-banking system. The literature review was conducted from the key words “*Operational Risk Assessment Methodology*”, “*E-banking Operational Risk Assessment Methodology*”, and “*Risk Assessment Methodology*”. The risk assessment methodologies covered the period of thirty eight years between 1977 and 2015. We included in the review papers which suggested a new risk assessment methodology covering at least one of the stages of a risk assessment process and where a method was specifically developed for or applied to an E-banking system. Finally, 8 papers, each presenting a risk assessment methodology, were selected for the analysis in this review paper. The methodologies were examined according to aim; application domain; stages of risk assessment addressed; risk impact analysis; sources of data for deriving probabilities; evaluation method and most importantly recommended tools for data analysis. The risk assessment methodologies and related

Scientia Africana, Vol. 19 (No. 3), December, 2020. Pp 101-124 https://dx.doi.org/10.4314/sa.v19i3.8
© Faculty of Science, University of Port Harcourt, Printed in Nigeria *ISSN 1118 – 1931*

works presented here are referred to by the author's name.

Summers's Methodology (Summers, 1977): Summers suggests an asset-oriented approach for conducting risk analysis. The method includes four major steps:

1. Identify assets and assign monetary values
2. Identify threats and vulnerabilities
   a. Estimate likelihood of occurrence for each threat
   b. Estimate impact of each threat
3. Calculate exposure of each asset to each threat
4. Identify potential safeguards and their costs

The analyst is first required to identify assets of the system and make a subjective but simplistic assignment of monetary values to each of the asset identified. The values can be assigned based on the values recorded in the asset register of the organization (known as standard accounting) or based on the replacement cost of the asset. However, the standard accounting approach is ideal for tangible assets, while the replacement cost approach is most suited for intangible assets (Vidalis, 2004). In calculating the output for this step, the values of security attributes (confidentiality, integrity, and availability) are also included. Next is the identification of possible threats and vulnerabilities. Probabilities are used for estimating the likelihood of each threat. The goal is to try to predict the importance / severity of each threat towards the system. The impact of each threat is calculated from the financial aspect using the following formula:

$$F(I) = \left[f(A) + f(In) + f(C) \right] \times f(L) \qquad (1)$$

Where I = threat impact, A = availability, In integrity, C = confidentiality and L = likelihood. The threats and vulnerabilities are linked by calculating the exposure of each asset to each threat. Finally the potential safeguards are identified. No metrics is however given to objectively identify these parameters and probabilities are being used for estimating the likelihood of each threat. There may be other non-financial but important long-term impacts organizations may be concerned about. Threat agents may defy probabilistic rules and equations; as humans are proven to be unpredictable and difficult to understand (Vidalis, 2004).

Carroll's Methodology (Carroll, 1996): Four main steps for conducting risk assessment was identified and includes

1. Threat assessment
   a. Likelihood estimation
   b. Severity prediction
2. Asset evaluation (importance, exposure, attractiveness)
   a. Vulnerability assessment
3. Impact assessment
   a. Threat and asset interaction
4. Safeguard evaluation

The methodology uses historical data for threat assessment and shows in the assessment process the methods used for identifying threat, threat agents and safeguards. The methodology assumes that an attacker must have the capability to perform the attack, the motivation and the opportunity to do so in order to manifest a threat. As a result a distinction is made between deliberate threats and accidental threats. Each threat is assessed based on two properties: likelihood and severity. Likelihood is evaluated as the number of occurrences of the threat per year, while severity refers to the consequences of the realisation of the threat. Next is asset evaluation, which is dependent on three factors: how important the asset is to the organization, its exposure, and its attractiveness. Lastly controls (safeguards) implemented or planned are evaluated.

This methodology fails to appoint the threat agent investigation and how to identify threat (Vidalis, 2004). In addition a major drawback to this method is that it requires the sole reliance on historical data for identifying and making future prediction on risks. It is not an appropriate approach for today's un-predictive and ever changing technological ways of conducting business especially in the context of E-banking.

Pfleeger's Methodology (Pfleeger, 1997): suggests an asset-oriented approach. The methodology uses five distinct information sources for calculating the risk such as; (a) probability estimate from observed data of the general population, (b) probability estimate from observed data for a specific system, (c) estimates of the number of occurrences in a given time period, (d) estimates of the likelihood from a table, and (e) the use of DELPHI approach. The methodology comprises of six major steps and includes:

1. Identify assets,
2. Determine vulnerabilities,
3. Estimate likelihood,
4. Compute expected annual loss,
5. Survey applicable controls and their costs
6. Project annual savings of controls.

It uses a subjective table in calculating the likelihood based on the frequency of the threat occurrence. The assumption is that when vulnerabilities are exploited, certain loss will be seen, and as a result annual loss expectancy is calculated by multiplying the loss due to vulnerability exploitation with the number of occurrences of the incident (Pfleeger, 1997). The method is likelihood estimation sensitive. However, Pfleeger's methodology is time consuming, which may render the results unusable. Data from other systems is not usable; as the methodology is based on the frequency of threat occurrences to a specific system.

Tanampasidis Methodology (2008): Tanampasidis proposed a methodology for assessing E-banking operational risk, which uses a Key Risk Indicator, 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

1. Strategy analysis and evaluation
2. Risk identification
3. Identification of points of risk mitigation and control
4. Risk evaluation
5. Risk measurement
    a. Business unit activity
    b. Application / subsystem functionality and constraints
    c. Identification of key risk factors
    d. Self-assessment
    e. Data processing
6. Reports.

The bank's strategic goals in the context of E-banking must first be described and documented by the auditor. Key bank executives are then interviewed by the auditor to determine the goal, corporate governance and policies. All operational risks associated with the key functions / services of the bank's E-banking system, without taking into consideration controls and points of mitigation, which may have been applied to reduce risk exposures (inherent risk), and all business units involved in the daily conduct of the E-banking process must be listed. The use of Strength Weakness Opportunity Threats (SWOT) analysis technique is suggested for identifying the level of operational risk to which the bank is exposed. Next, risk mitigation and controls applied by the banks are reviewed by the auditor to assess the quality of the allocated resources and costs. Previously identified risks are evaluated to determine the level of residual risk, after all controls are in place and their effectiveness level determined. The resulting output is a list of all the key risks to which the bank is exposed, the major control mechanisms / point of risk mitigation that was applied for risk exposure reduction. Thereafter, the risk related to the technical infrastructure is measured using Technical Infrastructure Risk Assessment Form (TIRAF). The average rate per Key Risk Factors (KRF) and per application / subsystem is calculated by the business units and the total. The resulting output is the measurement of risk related to the technical infrastructure. Finally, the auditor quantifies the average risk per KRF, average risk per function and the average risk per piece of technical infrastructure. Eventually the various outputs are summarized and documented for monitoring after the risks is analysed and evaluated. Several forms are used as tools for the information gathering process such as Business unit activity form and application description form which are used for identifying KRF and the major business processes Risk Assessment Form (RAF), which is used for self-assessing the level of risk exposures. The overall risk assessment process is based on expert opinion. 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. The idea is that business users may conceal some of the information or risk relevant for the evaluation from the analyst or auditor. Thus, 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 KRFs, thus results are not comparable to other similar surveys or even previous surveys in the same organization. KRIs cannot take into account process changes and system upgrades. Selecting the most relevant statistics to construct the KRIs, and the need to periodically maintain their relevance are the main challenges with KRI approaches, as some of the indicators may become obsolete due to changes in operational risk events (Adusei-Poku, 2005; Institute of Operational Risk, 2010). Further, KRIs are often incomplete or inaccurate in specification, there is no alignment between risk, KRI description and KRI metrics

Caralli et al. Methodology (Caralli et al., 2010): They proposed an Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) methodology to optimise the process of assessing information security risks. The goal is to allow broad assessment of an organization's operational risk environment by producing more robust results without the need for extensive risk assessment knowledge. The methodology comprises of eight steps that are organized into four different phases: establish drivers, profile asset, identify threats, and identify and mitigate risks. The steps include

1. Establish risk measurement criteria
2. Develop information asset profile
3. Identify information asset containers
4. Identify areas of concern
5. Identify threat scenarios
6. Identify risks
7. Analyse risks
8. Select mitigation approach

Set of qualitative risk measurement criteria are first developed and captured, to reflect the organizational drivers. These drivers will be used to evaluate the effect of a risk to the organization mission and business objectives. The risk measurement criteria form the foundation of the information asset risk assessment process. The resulting output of this step is the evaluation of the extent of an impact in a specific area and the impact areas that are most significant to its mission and business objectives. Next, a complete profile of the information assets is created. The most significant information assets are then identified, taking into consideration the containers in which the information assets live and the custodians of those containers. All of the points at which the information assets might be vulnerable to disclosure, modification, loss/ destruction, or interruption are also identified. This process forms the basis for threats and risks identification. Next, a brainstorming and characterization of the areas of concern are carried out to capture quickly those situations or conditions that could threaten the organizations' information asset. These areas of concern are then expanded into threat scenarios to further detail the properties of a threat. However, this process does not provide all the possible threats to the organization's information asset. As a result, they suggest that a robust range of possible threats be obtained by including other threat scenarios that were not identified while capturing the areas of concern. This process is carried out by using a threat tree structure that takes into consideration the asset, access/means, the various actors, motives, and outcomes inherent in the area of concern. Finally, risks are identified by considering the consequences possible threats will have on the organization if a threat scenario is realized. The goal is to try to predict the importance/severity of each threat towards the information asset. To identify the risks an organization is exposed to, a risk equation is used:

$$Threat\left(condition\right) + \text{Impact}\left(consequence\right) = Risk \quad (2)$$

Probabilities are used for measuring the likelihood of threat scenario and the impact of each threat. Further, an impact value is derived from the risk measurement criteria to measure the extent of a threat impact on the organization, by computing a risk score for each risk to each information asset. The relative risk score for each risk is determined by considering the severity of a risk outcome on the organization compared to the relative importance of the various impact areas. To compute the score for each impact area the impact area rank (using numerical ranking values) is multiplied by the impact value (qualitative values) and recorded in a score column. The total score for each column is equal to the total relative risk score. The relative risk score is computed in order to analyse identified risks and to help the organization determine an appropriate risk strategy.

Scientia Africana, Vol. 19 (No. 3), December, 2020. Pp 101-124 https://dx.doi.org/10.4314/sa.v19i3.8
© Faculty of Science, University of Port Harcourt, Printed in Nigeria *ISSN 1118 – 1931*

To select a risk mitigation approach, risks are prioritized (say from highest to lowest) based on their relative risk score. Risk with the highest score maybe considered first and categorized as mitigate or lowest as accept. A relative risk matrix which uses probability may be considered appropriate based on the organization needs. However, mitigation strategies are often decided by considering other factors such as the value of the asset and its security requirements, the containers in which it lives, and the organization's operating environment, cost, and benefits of mitigation strategy.

ARMS Working Group Methodology (ARMS Working Group, 2010): The ARMS working group proposed an operational risk assessment methodology for flight safety risk assessment. The methodology comprises three different phases and includes

1. Event risk classification (ERC)
   a. Risks assess all incoming events to be risk assessed (from safety reports, flight data events, safety survey results, audits etc.)
   b. Conduct preliminary database screening
   c. Store events in a safety event database
2. Data analysis
   a. Hazard identification from database
   b. Identify safety issues
   c. Assess identified safety issues
      i. Use Safety Issue Risk Assessment (SIRA) technique
      ii. Define and scope the safety issue before assessing risk
      iii. Calculate risk using prevention, avoidance, recovery and minimisation of losses factors
      iv. Determine the level of risk
3. Periodic safety assessments on new or revised operational activity

The Event Risk Classification phase is a process which requires a preliminary screening of the database within a very short period of time; say one or two days in order to identify any event occurrences and safety hazards requiring immediate action. This process is based on the concept of assessing the risk associated with one event and not the risk associated with all similar events. The output of the ERC process is both a risk class, which indicate the necessary actions needed for the risk inherent in the event, and a numerical value of risk, which can be used for quantification during the risk analysis phase. The findings of the ERC process are usually stored in a safety event database for further risk assessment, at a later specified time period. In order to identify a number of safety issues affecting the organization, the output of the ERC process is further analyzed along other data collected from other sources such as safety reports, questionnaire / surveys, external information and so on. Once the safety issues are identified, scenarios are created to identify the highest risk, which becomes the safety issue risk value. This safety issue is then calculated as the product of four factors: frequency/probability of triggering event, effectiveness of avoidance barriers, effectiveness of recovery barriers, and severity of the most probable accident outcome. These four factors expand upon the classical risk assessment formula (*severity x likelihood*) and together determines the risk exposure level. Frequency here refers to frequency of the triggering event, while severity refers to the severity of the potential accident outcome and not the severity of some intermediate outcome. In effect, the frequency of triggering event, the effectiveness of avoidance barriers, and the effectiveness of recovery barriers are assigned estimated numerical values or classes. These values or classes commonly defines the mean frequency of the accident due to safety issue, while the severity of the most probable accident outcome indicates the estimated severity of the potential accident to determine the risk. A factor of 10 of difference is used between the barriers effectiveness classes (e.g. the barrier will fail "once in 100 times", or "once in 10 times"). However, the frequency of triggering event is an estimate of the exposure of this event. The concept here is that the meaning of frequency and severity becomes clear when compared with the classical risk formula and that effectiveness of both avoidance and recovery barriers will allow the integration of the impact of controls in the risk assessment process. The third phase involves a periodic assessment of a specific part of the operation. They refer to this phase as the safety assessments process. The goal is to assess whether that part of the operation is safe enough, i.e. whether the risk level is acceptable. This process is focused on a new or changing part of the operation and the purpose is to ensure that planned operation will be safe. In conducting the safety assessment, the analyst is required to identify and analyse the associated hazards. The SIRA technique is then used to assess the risks related to the identified hazards. Although, they indicated that it may be impossible to use the SIRA framework when there are not enough factual and quantifiable elements to produce the SIRA, it can however be solved by using qualitative assessment that is based on domain expert judgments.

Although the objective of ARMS methodology is to provide an end-to-end risk assessment process, that can help reduce subjectivity inherent in current risk assessment methods, it however failed to identify the importance of including in the assessment, the cost for the occurrence of UOS or the system's value. In addition it failed to include in the assessment process the approximate cost for each occurrence of the threat-source's exercising the vulnerability (triggering events) in the assessment as suggested by National Institute of Standards and Technology (2002 & 2011).

NIST SP 800-30 Methodology (National Institute of Standards and Technology, 2011b**):** They proposed a general risk assessment methodology which encompasses nine steps:

1. System characterization
2. Threat identification
3. Vulnerability identification
4. Control analysis
5. Likelihood determination
6. Impact analysis
7. Risk determination
8. Control recommendation and
9. Results documentation.

The risk assessment process starts with the system characterization by defining clearly the scope of the effort, boundaries, available resources and the information contained in the system. Steps 2, 3, 4 and 6 can be conducted in parallel after step 1 is completed. Two distinct parameters: *impact* (also referred to as severity) and *likelihood* are used. Impact is described in terms of types of harm such as the harm to operations, assets, individuals, other organizations and the harm to the nation. To determine the overall likelihood rating for

Scientia Africana, Vol. 19 (No. 3), December, 2020. Pp 101-124 https://dx.doi.org/10.4314/sa.v19i3.8
© Faculty of Science, University of Port Harcourt, Printed in Nigeria *ISSN 1118 – 1931*

the probability that a potential threat source may exploit a given potential vulnerability, the analyst must make a subjective assignment of values based on the threat source motivation and capability, the nature of vulnerability, and the effectiveness of existing controls. In order to determine the adverse impact assuming a successful threat exercises or will exercise a given vulnerability, a risk scale and a risk-level matrix must be developed for measuring the risk level. The risk level scale can be a 3 x 3 matrix, 4 x 4 matrix, or a 5 x 5 matrix. The probability assigned to threats with overall ratings between 100 and 50 (exclusive) are classified as high risk, between 50 and 10 (exclusive) are classified as medium risk, and between 10 and 1 are classified as low risk. The risk is then derived by multiplying the assigned ratings of the threat likelihood and the threat impact. These parameters can be qualitatively (categories) or quantitatively (numbers) rated based on the information or data availability, and the exact formula is:

$$Risk = impact \times likelihood \qquad (3)$$

The goal is to determine the level of risk. In determining the risk, they assume that at certainty (i.e. 100% probability), the risk level equals the impact level. Each risk corresponds to a specific threat event with a level of impact if that event occurs. Thus, the general idea is that the risk level is typically not higher than the impact level, and the likelihood can serve to reduce the risk below the impact level. However, the upper bound on the risk analysis being equal to impact level at certainty may not hold for organizations with wide risk management issues, due to the potential for aggregation of risk. Further, even when each of the risk is at the moderate risk level, the aggregation of those moderate risk levels could aggregate to a higher risk level when multiple risks materializes. To solve these problems, they suggest that organizations could define a threat event as multiple occurrences of harm and an impact level associated with the cumulative degree of harm.

However, this method uses the classical risk score by multiplying the likelihood score with the severity of impact score. A major limitation or drawback to this approach 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 probability assigned to threats with overall ratings between 100 and 50 (exclusive) are classified as high risk, between 50 and 10 (exclusive) are classified as medium risk, and between 10 and 1 are classified as low riskthe risk respectively. By this standard risk scores there is no room for over lapping classification as seen in real life human-like subjective judgment.

Sousa et al. Methodology (Sousa et al., 2015): They proposed a methodology to minimize operational/technical risk across different processes or departments and also minimizing the possibility of spending excessive resources in a given process while other processes pose bigger risks to the organization or considered system. Their methodology comprises eight different stages and includes

1. Identify the system and its key processes. For each key process, stages 2-7 must be followed:
2. Identify process outcomes and respective internal events that result in process failure.

3. Select the dominant event in terms of impact in the results.
4. Estimate the consequence of process failure for the selected event.
5. Collect data about the occurrence of the event
    a. Identify controllable factors that influence process failure or the event occurrence
    b. Collect historical data about the occurrence of the event.
6. Select a model to fit data
    a. Conduct preliminary analysis of data
    b. Estimate model parameters
    c. Validate the model.
7. Use the model to
    a. Compute the probability of failure
    b. Compute process risk based on the dominant event
    c. Simulate changes in controllable factors to put process risk at a desirable level.
8. Analyze data to reduce the level of the internal risk of the considered system.

They suggest the use of Failure Mode and Effect Analysis (FMEA) in selecting the dominant event which has a higher impact on the system. The consequences of process failure can be estimated based on cost, as this will enable the decision makers to ascertain if further investment is needed to reduce the failure probability or the consequence. Once each key processes, respective risk and associated controllable factor(s) has been calculated, the decision makers are expected to analyze the data to reduce the level of the internal risk and also taking actions in controllable factors across all key processes associated higher risk. However, their proposed methodology requires the existence of historical data to estimate the probabilities of process failure.

Most of the traditional methodologies reviewed are highly subjective. The main problem with these traditional measurement approaches is that, they try to assess the *likelihood of a similar* risk event taking place in the future, rather than trying to assess the risk present in the event as it unfolded. In addition majority of the exiting approaches do not take into consideration the existing or potential risk controls into the assessment process in the proper manner. These approaches requires a relative long time span of historical data, but when applied in the context of E-banking it become even more difficult, as it is a relatively new area with little or no historical loss events. Further the role of infrequent but very large loss events occurrences, the internal controls and its ever changing nature, makes historical loss data somehow irrelevant.

Bayesian Network

Bayesian Network was first introduced by Pearls in 1988, as one of the most plausible inference classifier that is capable of representing conditional independencies (Adusei-Poku, 2005). Bayesian networks are capable of estimating missing information/data, and in conjunction with other BN statistical techniques or models, are able to combine domain knowledge and data to compute more quickly and effectively causal relationships between risk attributes, while effectively avoiding the problems of data over fitting (Heckerman, 1996; Adusei-Poku, 2005).

Definition of BN is given by Heckerman (1996) as a set of random variables **X**

Scientia Africana, Vol. 19 (No. 3), December, 2020. Pp 101-124 https://dx.doi.org/10.4314/sa.v19i3.8
© Faculty of Science, University of Port Harcourt, Printed in Nigeria *ISSN 1118 – 1931*

$=\{X_1,...,X_n\}$ which consists of a network structure S and a connected network of nodes corresponding to the random variables in **X**, and a set of ***P*** of local probability distributions associated with each variable. Together, these components define the joint probability distribution function (*PDF)* for **X**. The network structure ***S*** must be a Directed Acyclic Graph (*DAG*) and the nodes in ***S*** are in one-to-one correspondence with the variables.

If we let X_i denote both variable and its corresponding node, and let Pa_i denote the parents of node X_i in ***S*** as well as the variables corresponding to those parents, then given structure ***S***, the joint *PDF* for **X** can be calculated as:

$$p(x_i \mid x_i,...,x_{i-1}) = p(x_i \mid \pi_i) \qquad (4)$$

The local probability distributions ***P*** are the distributions corresponding to the terms in the product of equation 4. Consequently, the pair (***S***, ***P***) encodes the joint distribution *p*(x).

Bayesian Networks can be constructed into a "multi-level" model, which can show several levels of dependency among several risk factors (e.g. frequency of outsider fraud attacks as a result of successful Trojan attacks on a customer's computer, which is also enhanced by the weaknesses of the bank IT systems, such as the cryptographic techniques).

Bayesian Networks have been applied on a wide range of fields such as: medical and mechanical diagnosis, in ecology, data mining and intelligent trouble shooting systems, risk and reliability assessment, financial risk management, image modelling, genetics, speech recognition, space exploration and powerful web search engines. In risk and reliability assessment, Philips Consumer Electronics uses BN technology to predict software defects in its consumer electronics (Fenton et al., 2001). Some examples in financial risk management include the credit risk prediction tool *BayesCredit* and the *iRisk* tool for operational risk prediction (Neil et al 2005).

Fuzzy Logic

Fuzzy logic has been used for decades in the engineering sciences to embed expert knowledge into computer models for a broad range of applications (Aburrous et al., 2010). Lotfi Zadeh in the mid-1960s developed fuzzy logic 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). The logical facet of fuzzy logic is focused on logical systems in which truth is a matter of degree – a degree which is allowed to be a fuzzy set (Zadeh, 2004). Zadeh (1992) 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 the fuzzy set theory, fuzzy set A of universe X is defined by function $\mu_A(x)$ called the membership function of set A

$$\mu_A(x): X \to [0,1], \qquad (5)$$

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. With logical operations on fuzzy sets, inference rules can be built to establish the relationship among different variables.

Fuzzy Inference System also known as fuzzy-rule-based system, fuzzy expert system, fuzzy model, fuzzy associative memory, fuzzy logic controller, and simply but ambiguous, fuzzy system (Negoita et al., 2005), is a computing framework that provides a robust approach to deal with uncertainty and vagueness and it is based on the concepts of fuzzy set theory, fuzzy reasoning, and fuzzy rules (Jang et al., 1997). It uses the mathematical theory of fuzzy sets in simulating the process of normal human reasoning and represent fuzzy truth membership in vaguely defined sets, such as the likelihood of some event or condition (Jang et al., 1997). FIS are capable of providing high degree of flexibility in classifying data and are able to incorporate expert domain knowledge to define variables and their relationships.

In other words, fuzzy logic rule-based induction can be used to handle inconsistent and missing data, by aggregating the hypothesis of all the rules (Dunham, 2003; Negoita et al., 2005; Vargas, 2009; Venugopal et al., 2009). Several fuzzy rules may be used simultaneously to produce outputs, and the outputs are usually represented by fuzzy sets (Vargas, 2009). The reasoning behind this approach is that decision making is not always a classical logic; it often involves unstructured and vague variables. Further, in data mining the extraction and processing of qualitative attributes can become very complex and difficult by applying conventional rule induction techniques (Venugopal et al., 2009).

PROPOSED E-BANKING ORA METHODOLOGY

In this section we will present our methodology for improving the assessment of E-banking operational risk. In the context of this research the ARMS methodology was extended and used as a guideline as it employs the principles of both the ISO / IEC 31010:2009 and ISO / FDIS 31000:2009 standards. The methodology also provides a forward-looking risk assessment methodology needed to identify triggering events and frequency of occurrences, effectiveness of both preventive and detective controls, as well as the impact of risk that events carry as it occurs within the E-banking operation. The proposed risk assessment methodology consists of four major steps: a risk model, assessment approach, analysis approach and a risk assessment process. The main tool of the proposed risk assessment methodology is the risk assessment process. The risk assessment process is built upon fuzzy logic concept and Bayesian network. Our proposed E-banking ORA methodology is discussed by first defining the risk model, the assessment approach and the analysis approach.

Risk Model

Scientia Africana, Vol. 19 (No. 3), December, 2020. Pp 101-124 https://dx.doi.org/10.4314/sa.v19i3.8
© Faculty of Science, University of Port Harcourt, Printed in Nigeria *ISSN 1118 – 1931*

A risk model is the key terms used in risk assessments, the risk factors to be assessed and the relationships between those risk factors. That is the risk attributes such as threats, vulnerabilities, threat agents, other risk factors, and their relationships (National Institute of Standards and Technology, 2011b). Defining clearly the risk model will help the organizations or the analysts, to understand significant dependencies and effectively determine the risk inherent in their problem domain. Figure 1 illustrates our proposed operational risk model.

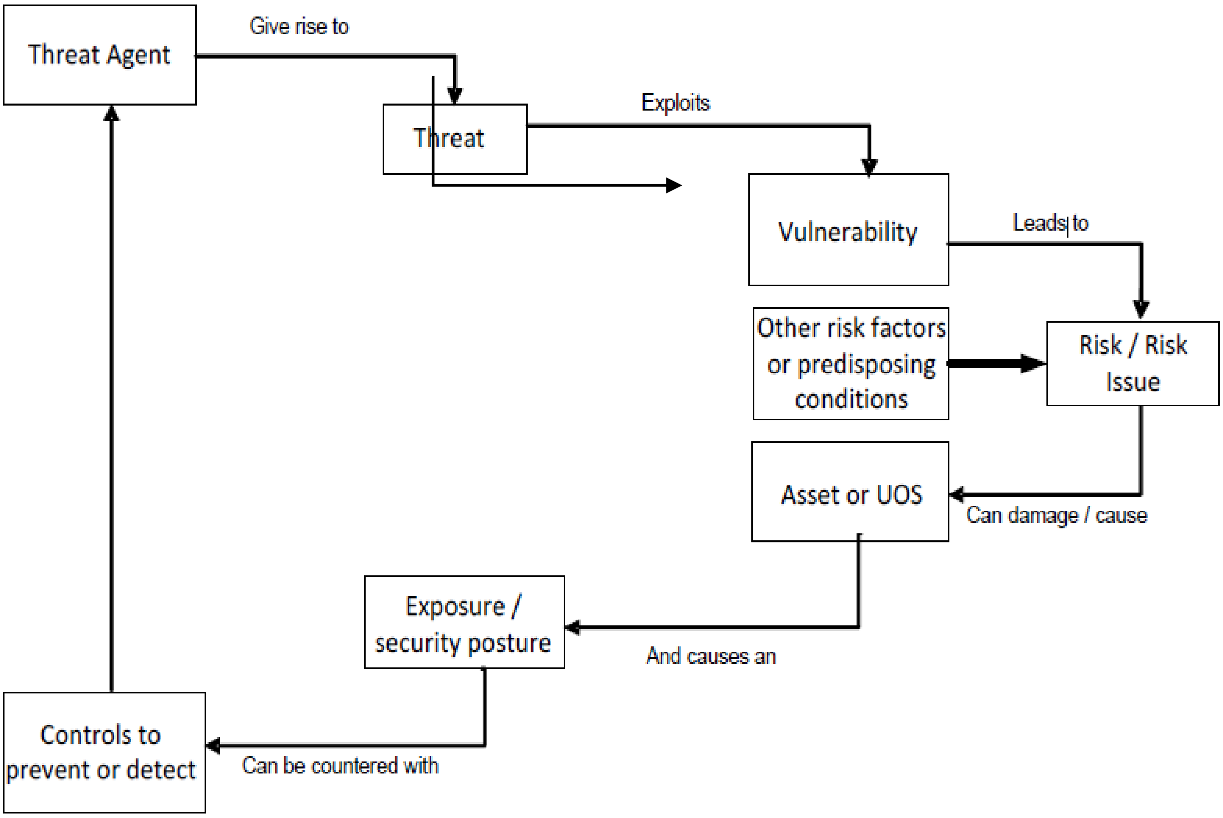

Figure 1. Proposed E-banking OR Model

A threat agent with the capability and intent could give rise to threat events by exploiting the system vulnerabilities such as software vulnerability (e.g. authentication and authorization process for example two password authentication only), network vulnerability (e.g. Modem, FTP, DoS), hardware failures, etc., which could lead to a risk or risk issues with a likelihood of occurrence. These risks or risk issues could damage an asset or cause an undesirable operational state (UOS) with an impact, and thus causing risk exposures on the system or the organization as a whole. However, risk exposure levels are determined by the effectiveness level of the controls in place to both prevent and recover the asset against threat agents.

Risk Assessment Approach

The consensus is that organizations may employ qualitative, quantitative, or semi-quantitative risk assessment approaches based on risk criteria, risk appetite and organizational culture, availability of data/analysis expertise of the organizations and the decision-making needs of the organization (Sadiq et al., 2007; BSI, 2010; National Institute of Standards and Technology, 2011b). Some of the approaches and degree of details may be prescribed by legislation. However, it is important the organizations or analysts understand the advantages and disadvantages of deploying their preferred approach.

In this research, we propose the semi-quantitative approach for measuring E-banking OR, due to the difficulty of quantifying operational risk, the role of infrequent but very large loss events occurrences, which makes historical loss data somehow irrelevant. Moreover, the definition of risk "*risk is a state of uncertainty when a given threat source exploits one or several vulnerabilities, resulting in an adverse or non-adversarial impact, where some of the possibilities involve a loss or other undesirable outcome*" (Hubbard, 2010; ISO, 2011), means that calculating risk on quantitative or qualitative data alone, may lead to highly subjective and unrealistic risk values, for example when historical data are scarce or when the variables are too biased towards experts level of knowledge.

Semi-quantitative approaches use a set of methods, principles or rules that uses bins or numerical rating scales for representing consequences and probabilities, and produces the level of risk by combining these using a formula for assessing risk. Scales may be linear or logarithmic, or have some other relationship. These scales or bins translate easily into qualitative terms which help in supporting risk communications for decision makers. Formulae used in this approach may vary, and expert judgement in assigning values is more evident in the semi-quantitative approach than in a quantitative approach (BSI, 2010; National Institute of Standards and Technology, 2011b). However, rigour is significantly reduced when subjective determinations are contained within assessments, or when significant uncertainties are present in the determination of values. When bin or scales rating are embedded in the assessment, care must be taken to ensure that they are not attributed a level of accuracy and precision inconsistent with the accuracy of the data and methods employed. Thus, clear meaningful examples of the bins or ranges of scale must be defined or characterised (BSI, 2010; National Institute of Standards and Technology, 2011b).

Risk Analysis Approach

Risk analysis approaches are determine by the starting point of any risk assessment process, the level of details required in the assessment and how risks will be treated. Basically there are six risk analysis approaches: preliminary/database screening, threat-oriented, vulnerability-oriented, asset/impact-oriented, graph-based analysis, and rigorous analysis (ARMS Working Group, 2010; National Institute of Standards and Technology, 2011b). However, an organization or an analyst may choose any of the approaches or a combination (National Institute of Standards and Technology, 2011). In this research we propose the use of the Preliminary/database screening and graph-based analysis approaches. The suggestion is that Fuzzy Inference System could aid the establishment of the context domain area (i.e. identify the type of E-banking system to be considered for assessment). Preliminary/database screening approach

Scientia Africana, Vol. 19 (No. 3), December, 2020. Pp 101-124 https://dx.doi.org/10.4314/sa.v19i3.8
© Faculty of Science, University of Port Harcourt, Printed in Nigeria *ISSN 1118 – 1931*

should be adopted by either using factor analysis or other statistical technique for screening the dataset, in order to identify the most significant risk attributes on the E-banking system under study, thus ensuring resources are focused on the most important operational risks for further risk assessment. The graph-based analysis approach should then be adopted by using the Tree Augmented Naïve Bayes classifier, in identifying the triggering factors to operational risk and their causal relationships from this screened dataset. Finally, the Fuzzy Inference System should be used in determining the OR exposure levels inherent in the E-banking system under study. These approaches are considered appropriate because of how well they are able to incorporate internal / external data, scenarios, BEICFs approach, to modelling the causal relationships between risk factors, key risk indicators and other domain attributes in the risk analysis and determining the inherent risk exposures.

Risk Assessment Process

Risk assessment process involves the identification of risk, analysis of risk, and evaluation of risk (ISO, 2005; Standards Association of Australia, 1999; National Institute of Standards and Technology, 2011a; ISO, 2011). The ISO / IEC 27001:2005 provides a sequencing of the core part of the risk assessment process into sub-processes for context identification, risk identification, risk analysis and risk evaluation (ISO, 2005). Figure 2 and 3 shows the general risk assessment contribution to risk management process and a detailed risk assessment process respectively.

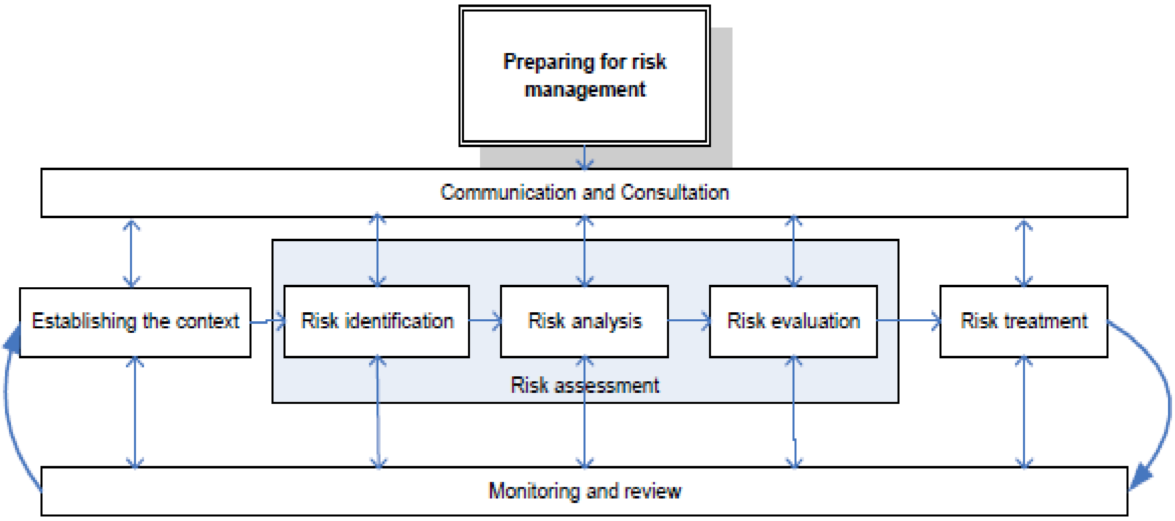

Figure 2. General risk assessment contributions to risk management process

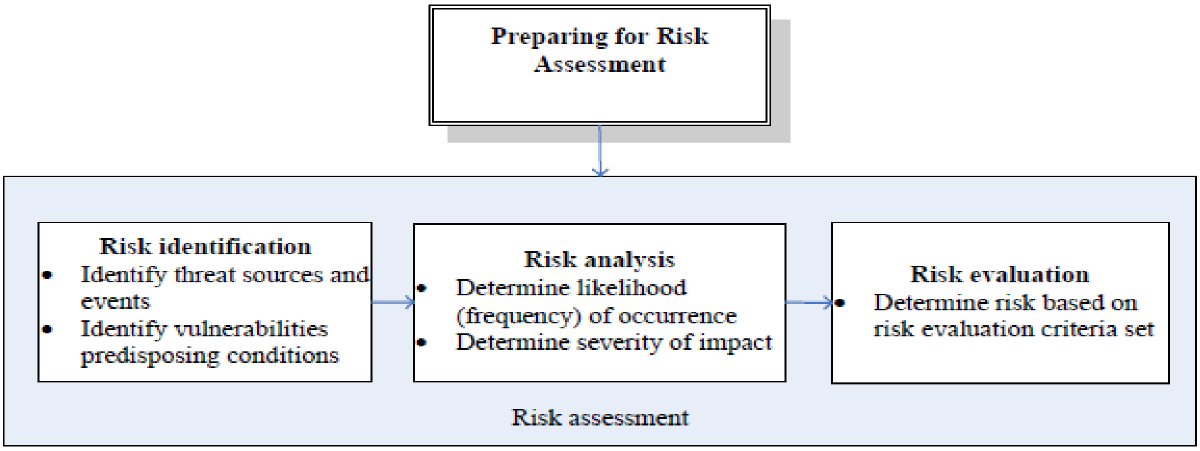
Preparing for Risk Assessment
Risk identification
Identify threat sources and events
Identify vulnerabilities predisposing conditions
Risk analysis
Determine likelihood (frequency) of occurrence
Determine severity of impact
Risk evaluation
Determine risk based on risk evaluation criteria set
Risk assessment

Figure 3. A Detailed Risk Assessment Process

The first step in the risk assessment process is to prepare for the assessment, by establishing the context for the risk assessment. That is defining clearly the system or information asset that will be risk assessed. This context should be established and informed by the risk management strategy of the organization that was developed during the risk framing step of the risk management process. Thereafter the scope, purpose, boundaries of the system, along with the resources and information that constitute the system or asset must be identified.

The general consensus is that traditional banking risk assessment and management principles, tools and techniques are applicable to E-banking activities (Basel Committee on Banking Supervision, 2003). In this study the general risk assessment process is extended based upon the ARMS Working Group risk assessment methodology (ARMS Working Group, 2010) and the NIST Special Publication 800-30 revision 1 guide for conducting risk assessments (National Institute of Standards and Technology, 2011b). The proposed E-banking OR assessment methodology gives detailed explanation with respect to which models or techniques may be applied and how they are expressed. Although, the sub-processes are sequenced the E-banking OR assessment methodology is iterative and allows feedback. The proposed OR assessment methodology consists of five major steps and includes

1. System Characterization/Asset Identification
2. Risk Identification
   a. Threat identification
   b. Vulnerabilities identification
   c. Other background information identification
   d. Conduct preliminary screening of information in a, b, and c (using factor analysis for example)
      i. Identify risks that require urgent actions
      ii. Make recommendation for immediate risk mitigation
      iii. Store identified risks in the risk event database
3. Data analysis (using Bayesian network and fuzzy logic)
   a. Identify risk issues from databases / datasets
   b. Use ORA framework
      i. Define and scope the risk issue before risk assessing
      ii. Identify triggering risk events

   iii. Identify avoidance and recovery barriers (controls)
   iv. Identify UOS and cost
   v. Identify severity of the risk outcome
  c. Calculate risk using the ORA formula
   i. Frequency/probability of the so-called triggering events
   ii. Effectiveness of the avoidance barriers (controls)
   iii. Frequency of UOS occurrences
   iv. Effectiveness of the recovery barriers (controls)
   v. Cost of UOS occurrences
   vi. Severity of the most probable risk outcome
  d. Determine the level of risk
4. Evaluate risk
  a. Use estimated risk exposure level portfolio
  b. Identify risk criteria defined during context establishment
  c. Identify significance of the level and type of risks
  d. Identify risk scale values, definitions and required actions
   i. Make control recommendation on decisions to accept, treat, monitor or review risk.
5. Results documentation and recommendations

System Characterization/Asset Identification

The first step in the risk assessment process is to prepare for the assessment, by establishing the context for the risk assessment. That is defining clearly the system or information asset that will be risk assessed. This context should be established and informed by the risk management strategy of the organization that was developed during the risk framing step of the risk management process. Thereafter the scope, purpose, boundaries of the E-banking system, along with the resources and information that constitute the system or asset must be identified. System characterization or asset identification is compulsory; as it helps to establish the scope of the assessment effort, provide information essential to defining the risk and delineates the operational authorization boundaries.

Several information gathering techniques such as questionnaire, interviews, document review, and automated scanning tools are available, and can be used for identifying the system of interest and its operational boundary. Any, or a combination of these techniques can be employed.

Risk Identification

Risks should be identified by first assessing the underlying E-banking operations against the potential threats, vulnerabilities, and other background information that may impact upon objectives. The goal of this step is to identify and list the potential threat sources/agents, their motivations and threat events applicable to the E-banking system being evaluated. At this stage it is important to identify also vulnerabilities (weaknesses or flaws) that could be exploited by the potential threat agents.

Next, analysts should conduct a preliminary data screening of the information collected so far on threats, vulnerabilities and other background information that may impact upon the E-banking operation. This is to enable the identification of risks which requires immediate risk mitigation and to identify the most significant risks or to exclude less significant risk from further analysis at later specified date. Preliminary data analysis is necessary because it allows the organization to focus resources on the most significant risks.

There are several methods for identifying risk, including the evidenced based method, which requires comprehensive use of check-lists or historical data on threats, vulnerabilities, and threat events reported previously either in the database or literature. They can however be used at any stage of the risk assessment process (e.g. risk identification, control failures determination and so on). The outputs will however depend on the stage of the risk assessment process to which they are applied. The OCTAVE threat profile or any suited technique can also be used as a guide to creating a comprehensive list of threats, threat agents, and actions associated with the E-banking system being evaluated. The system vulnerabilities could be identified by using vulnerability sources (e.g. NIST I-CAT vulnerability database), the performance of system security testing (e.g. automated vulnerability scanning tool), and the development of a security requirements checklist.

A major benefit of using the check-list approach is that it can be used by non-experts. It allows for the combination of a well-designed range of expertise into an easy to use system and also able to ensure common problems are not forgotten. However, their limitations include but are not limited to the following: they encourage ‘tick the box’ type behaviour, tend to miss problems that are not readily seen due to their observational nature, and tend to inhibit imagination in the risk identification stage (British Standards Institution, 2010).

Another method for risk identification is referred to as the systematic team approach. It uses a structured set of prompt questions such as interviews and survey questionnaires for identifying risk. Interviews and questionnaires are often used to identify risks or to assess control effectiveness as part of a risk analysis process (British Standards Institution, 2010; Institute of Operational Risk, 2010). They may however be applied at any stage of the assessment process or project. In conducting interviews (structured or semi-structured) and survey questionnaires, relevant set of questions and interview objectives must be clearly defined by the analysts. This is to guide the interviewer and to allow a degree of flexibility in providing opportunity of exploring areas into which the interviewee may wish to go, which will prove essential for effective risk analysis. In addition, a well-defined list of interviewees or survey respondents must be selected from relevant stakeholders (British Standards Institution, 2010) or groups of people.

Some organizations have found benefits from using comprehensive and extensive standard questionnaires with questions allocated to respondents based upon the relevance of the activities (Institute of Operational Risk, 2010). However, it is time-consuming for the analysts to obtain multiple opinion or responses. It is biased tolerated and thus not removed from the discussion or responses, which may have significant impact on the risk analysis. The triggering of the imagination feature of the brainstorming technique may not be achieved (British Standards Institution, 2010) with these approaches. However, the interview and survey questionnaire approaches are useful where brainstorming is proven difficult to apply in the problem domain.

Finally, the initial assumptions and results of the risk analysis must be documented and stored in the organizations database, along with the identified E-banking risks, threats, threat agents and their motivations, and vulnerabilities. It is important to develop databases, which can be used for data analysis and where individual risk events can be found easily.

Data Analysis using Bayesian Network and Fuzzy Logic

The main purpose of data analysis is to identify risk issues affecting the E-banking operation, their causal relationships, implemented or planned controls effectiveness, and to determine the inherent risk exposure level and the residual risk from existing data. It is however important at this stage to carry out first a preliminary database/dataset screening of risk previously classified, in order to identify quickly risks that require immediate actions. Automatic scanning tools and techniques such as soft computing tools and other statistical data analysis tools (i.e. SPSS) may be used. Charts, graphs and filters may be produced to sort the risk events by different combinations. Results can be presented as "number of events" or "rate of events" and/or their causal relationships. The resulting output of the preliminary analysis should be used as input to identifying the most significant risk issues affecting the E-banking system under study and also to identifying the risks that highlight the need for immediate risk treatment. Bayesian network classifiers discussed in section 2.1 should then be deployed to determine their causal relationships across multiple events and identify the most significant risk issues.

Further, analysis should then be carried out on the most significant risk issues identified. These risk issues should be assessed using an ORA framework such as the one described in (Ochuko, 2012). At this point, fuzzy logic discussed in section 2.2 should be deployed on the chosen risk issue(s). These risks must be clearly defined and scoped. Triggering risk events, and controls to avoid and recover before risk outcomes should also be described. Based on the data collected analyst should highlight contributing factors and their frequency of occurrence to risk events. That is determine the specific conditions which existed when risk events occurred and how these conditions may have influenced the frequency and severity of loss to risk events. The analysis of controls effectiveness levels to both (prevent and recover before risk outcome) may be expressed qualitatively, semi-quantitatively or quantitatively. A formal review either by inspection or by statistical tests (that is sampling) could be performed and will inform the formal risk assessment process. However, this decision may be based on the rigor, available data format, analyst expertise and the RCSA process. Planned or implemented control analysis is necessary in determining risk, because control failures will tip the balance between inherent and residual risk, it will affect the severity of risk impact and thus may cause devastating financial and reputational effect on the E-banking system or the organization as a whole.

Consequence or risk outcome analysis determines the type and nature of impact risk event occurrences will have on the E-banking system. Analysis may be a simple description of risk outcomes to detailed quantitative analysis. Severity of the risk outcome or the most probable outcome must also be described. Defining the factors will enable the risk assessment more factual, because analyst can then create and calculate the risks and determine the level of risks inherent in the E-banking system.

The analysts must also identify the undesirable operational events they are trying to avoid. The question asked here does not refer to the most probable outcome or the worst case scenario but undesirable operational events that could create UOS which could in turn result in an accident or risk with an impact on the E-banking operation. Organization can characterize magnitude of impacts and UOS by security objective (e.g. loss of confidentiality, integrity, or availability). The approximate cost of UOS should be determined; as this will provide a good base for the valuation of assets and also help in identifying clearly the magnitude of risk impact.

Once the key risk issues, triggering events, controls implemented, several potential risk outcomes have been precisely defined around one or more UOS, the information should then be entered into the ORA framework and implemented using the fuzzy inference system. These factors should be calculated using the ORA formula which is calculated as a product of the six factors in equation 6, as shown in the Cartesian product:

Risk Exposure Level (*REL*) = *Triggering Events (TE)* x *Avoidance Barriers (AB)* x *Undesirable Operational State (UOS)* x *Cost of UOS* x *Recovery Barriers (RB)* x *Severity of Risk Outcome (SRO)* (6)

Estimate of the probable frequency / likelihood and the probable magnitude of impact associated with the E-banking risk scenarios; as influenced by applicable triggering events (risk factors) should be made. Finally, the analysts should determine the risk exposure level based on the most important risk scenarios and develop the effectiveness of identified controls (their capability to detect and to recover before risk outcome, and their effect on probable frequency and magnitude, and applicable risk factors). Equation (7) reveals that risk exposure level is simply the product of the ORA factors once they are assessed.

$$\mathrm{Re}l_{x_i} = \mathrm{F}_{te} \times FA_{uos} \times F_{uos} \times F_{rr} \times EC_{uos} \times S_{ro} \qquad (7)$$

Where $\mathrm{Re}l$ = 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.

Risk Evaluation

In this step, analysts should evaluate the risk based on the estimated risk exposure portfolio. At this stage the estimated levels of risk must be compared with the risk criteria defined during context establishment, in order to determine the significance of the level and type of risks. The meaning of each risk scale values, definitions and required actions must be clearly defined and agreed upon with top management or stakeholders of the organization. These decisions may include the need to treat, monitor or review risk. Decisions may also depend on the costs and benefits of taking the risk and the costs and benefits of implementing improved

Scientia Africana, Vol. 19 (No. 3), December, 2020. Pp 101-124 https://dx.doi.org/10.4314/sa.v19i3.8
© Faculty of Science, University of Port Harcourt, Printed in Nigeria *ISSN 1118 – 1931*

controls. Cost / benefit analysis are often used for evaluating risk. The estimated E-banking operational risks could be evaluated by dividing them into three bands (see British Standards Institution, 2010). These bands are:

1. An upper band where the level of risk is regarded as intolerable, where urgent risk treatment is required irrespective of the cost or the benefits the activity may bring.
2. A middle band where costs and benefits are taken into account by balancing opportunities against potential consequences.
3. A lower band where the level of risk is regarded as negligible, and as a result no risk treatment is necessary.

Result Documentation / Recommendations

The results of the risk assessment should be generated and documented based on; the information associated with the risk model, chosen risk assessment methodologies, analysis approaches, and the four stages of the ORA process proposed. Operational risks and other findings should be expressed in clear and understandable terms, in order to help the risk management team or top executives of the organization to monitor the risk assessment process and control effectiveness justification. However, the granularity of the report will depend on the objectives and scope of the assessment. It is important to include in the report, insights related to anticipated time frames associated with particular risks. Documentation can include also relevant parts of the system and their functions; assumptions and uncertainty analysis. Finally, conclusions and recommendations must be documented in accordance with the need of the risk management process. Periodic risk event and risk factor analysis, to identify new or emerging risk issues must be a carried out and updated on this on-going risk factors monitoring.

CONCLUSIONS / FUTURE WORKS

In this work we have proposed a new methodology based on fuzzy logic and Bayesian network for assessing E-banking operational risk. The Bayesian-Fuzzy based concept are capable and useful for analysing risks with incomplete data, uncertainty, and expert opinion and as a result give good predictions for risk learning and inference in such systems. The proposed methodology consist of four major steps: a risk assessment process, a risk model, assessment approach and an analysis approach. Concretely, this approach try to assess the risk present in the event, in order to identify the risks that highlight the need for immediate risk treatment as it unfolds, rather than try to assess the likelihood of a similar risk event taking place in the future. This research provides a forward-looking risk assessment methodology needed to identify triggering events and frequency of occurrences, effectiveness of both preventive and detective controls, as well as the impact of risk that events carry as it occurs within the E-banking operation.

The E-banking OR methodology is able to help risk assessment officers and E-banking system operators, identify variable dependencies as well as to understand drivers for E-banking risks; to understand customer’s fraudulent attacks experiences, severity and the frequency of such attacks, and customer’s perceptions on the banking institutions performance. The methodology is also able to help risks assessment officers

/ senior executives, to review and make predictions on their banking risk profile. Further technology adopters will also benefit from the risk assessment methodology, as they are able to assess the effects of possible interventions on their planned system adoption, as well as other organizational goal.

Future work will delve into the implementation procedure of the proposed methodology 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

Adusei-Poku, K. (2005) *Operational Risk Management-Implementing a Bayesian Network for Foreign Exchange and Money Market Settlement.* PhD thesis, University of Gottingen.

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

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

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

Caralli, R. A., Stevens, J. F., Young, L. R. and Wilson, W. R. (2010) *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*. Software Engineering Institute Technical Report: CMU/SEI-2007-TR-012, ESC-TR-2007-012

Carroll J. M. (1996) Computer Security, Butterworth-Heinemann.

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

Fenton, N. E., Krause, P., and Neil, M. (2001) A probabilistic model for software defect prediction. Submitted for publication in *IEEE Transactions in Software Engineering* [online]. Available from: http://www.eecs.qmul.ac.uk/~norman/papers/fenton_krause_neil_IEEE.pdf

Heckerman, D. (1996) *A Tutorial on Learning with Bayesian Networks*. Technical Report: 1996- MSR-TR-95-06.

Hubbard, D. W. (2010) *How to Measure Anything: Finding the Value of "Intangibles" in Business*. 2nd edn., New Jersey: John Wiley & Sons, Inc.

Institute of Operational Risk, (2010). *Operational Risk Sound Practice Guidance: Key Risk Indicators* [online]. Available from: www.ior-institute.org

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

International Organization for Standardization (2011) ISO / IEC 27005. *Information Technology –*

Scientia Africana, Vol. 19 (No. 3), December, 2020. Pp 101-124 https://dx.doi.org/10.4314/sa.v19i3.8
© Faculty of Science, University of Port Harcourt, Printed in Nigeria *ISSN 1118 – 1931*

Security Techniques – Information Security Risk Management. Geneva: International Organization for Standardization.

Jang, J. R., Sun, C., and Mizutani, E. (1997) *Neuro-Fuzzy and Soft Computing: A Computational Approach to Learning and Machine Intelligence*. Upper Saddle River, NJ: Prentice Hall.

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.

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.

Negoita, M., Neagu, D., and Palade, V. (2005) *Computational Intelligence: Engineering of Hybrid Systems*. Heidelberg: Springer-Verlag.

Neil, M., Fenton, N. E., and Tailor, M. (2005) Using Bayesian Networks to Model Expected and Unexpected Operational Losses. *Risk Analysis,* Vol. 25, No.4, pp963-972

Ochuko (2012) E-banking Operational Risk Assessment: A Soft Computing Approach in the Context of the Nigeria Banking Industry. PhD Thesis, University of Bradford.

Pfleeger C.P. (1997) Security in Computing, Prentice Hall Int.

Sadiq, R., Kleiner, Y., and Rajani, B. (2007) Water Quality Failures in Distribution Networks – Risk Analysis using Fuzzy Logic and Evidential Reasoning. *Risk Analysis*, Vol. 27, No.5, pp1381-1394.

Standards Association of Australia (1999) AS/NZS 4360:1999. *Risk Management*. Australia: Australian Standard.

Sousa, S., Nunes, E., and Lopes, I. (2015) Measuring and Managing Operational Risk in Industrial Processes. *Faculty of Mechanical Engineering Transactions*, Vol. 43, No.4, pp 295-302.

Summers, R.C. (1977) Secure Computing: Threats and Safeguards, McGraw-Hill.

Tanampasidis, G. (2008). A Comprehensive Method for Assessment of Operational Risk In E-banking. *International Systems Control Journal*, Vol. 4, pp1-7.

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

Venugopal, K. R., Srinivasa, K.G., and Patnaik, L. M. (2009) *Soft Computing for Data Mining Applications*. New York: Springer.

Vidalis, S. (2004) A Critical Discussion of Risk and Threat Analysis Methods and Methodologies. School of Computing Technical Report: CS-04-03.