Banking Information System: residual risks modeling

Marie NDAW
PHD Student, Mission Officer
ESP UCAD, GIM UEMOA, Senegal
marieelisaadam.ndaw@ucad.edu.sn

Gervais MENDY
PHD, Teacher
ESP, UCAD, Senegal
gervais.mendy@ucad.edu.sn

Samuel OUYA
PHD, Teacher
ESP, UCAD, Senegal
samuel.ouya@ucad.edu.sn

***Abstract*—Banking Products and services are more and more innovative using Internet and mobile technologies. For this reason, bank information system must be protected against several risks considering physical or logical attacks which can cause important financial losses. In this paper, we propose a quantification model of information system residual risks which are the risks remaining after the response of management. Our model provides an automatic calculation of security measures impact on information system risks and it is based on FMECA (Failure Modes and Effect Criticality Analysis Method) which is an inductive reasoning method studying causes, effects of failures and criticality. For testing, the values obtained with the model were compared to reference values given by assessors during different working sessions. The result is satisfactory, facilitates risk analysis, helps to maintain information system security, to increase banks profit and customers confidence.**

***Keywords*-Banking Information System, Residual Risk, Model, Security, Control**

I. Introduction

Risk is the potential harm that may arise from some current process or from some future event. Information system risk is a function of the likelihood of a given threat-sources and the resulting impact of that adverse event on the organization [1]. Threat is potential for a threat-source to exercise a specific vulnerability and threat-source is a situation that may accidentally trigger a vulnerability [2]. Bank information system has several risks considering the new products and services related to mobile and online banking. The potentials frauds have financial, commercial and juridical impacts. This implies decrease of bank profit and customers confidence. To manage their risks which can have major business impacts for the bank, it is necessary to inhibit threat, reduce and eliminate vulnerability, protect and move asset [3]. Risk management process has different steps including assessment, timing of exercise, consistency in approach and implementation [4]. It also includes cost-benefit analysis and selection, test and evaluation of safeguards. In that context, implementation of best practices should be consistent with the enterprise risk management and control framework, appropriate for the enterprise and integrated with other methods and practices that are being used [5]. Various security standards are proposed and concern different fields of information system:

- MEHARI: Risk analysis method and set of tools specifically designed for security management [6].
- COBIT: IT governance and framework of best practices in managing resources, infrastructures, processes, responsibilities and controls [7].
- ITIL: Library of good practices related to information technology services [8].
- ISO 27001: Methods and practices for implementing information security in organization [9].
- ISO 22301: Governance process supported by top management to implement and maintain business continuity management [10].

Banks implement many security measures to safe information and transactions. Nowadays, ATM (Automated Teller Machine) or POS (Point Of Sale) frauds, Internet banking frauds and fraudulent transfers or withdrawals contributed most to frauds in banking sector. For these reasons, banks must prevent fraud, improve product penetration, capture a substantial number of customers with little or no banking experience and attract more savers [11]. Also, the vendor should be knowledgeable about standards such as the PCI DSS (Payment Card Industry Payment Card Industry Data Security Standard) [12]. For online transactions, 3D-Secure is an adaptive authentication protocol enables merchants and issuers to other additional cardholder protection. Authentication is attempting to confirm that the person initiating a transaction is the legitimate and genuine cardholder [13]. Also, layers of security must be considered as the EMV (Europay Mastercard Visa) chip card adoption cycle matures. Ideally, each stakeholder should address fraud with their EMV chip migration strategy [14]. Merchants have to stem rising fraud losses, while issuers have to rein in fraud and also maintain consumer confidence in the security of online transactions [15]. Periodically, Banks assess the impact of those implemented controls on information system risks using an actual method which has some limits. This method is manual, requires time and personal investment and has some estimation error. So we propose to automatize the assessment of banking information system residual risks.

II. Related work

Information system risk is a function of the likelihood of a given threat-sources exercising a particular potential vulnerability and the resulting impact of that adverse event on the organization. Generally, risk assessment includes process of identifying the risks, determining probability of occurrence and resulting impact and additional safeguards that would mitigate this impact. Information system risk management allow implementation of appropriate controls in order to reduce or eliminate risks [16]. Different steps exist: determining the level of inherent risk, monitoring the effectiveness of the risk management practices, determining whether the residual risk is improving, stable or eroding over time [17]. Considering the actual banking products and services, the financial, payment and network service providers should implement the appropriate safeguards. Each bank should implement strong positive controls to protect such data while in its custody, identify personal and sensitive data and should ensure that appropriate mechanisms are in place [18]. Various risks have been associated to mobile payments like anti money laundering, credit, liquidity, fraud and compliance [19]. The strategic risk with mobile payments is of an attack that makes fraud so easy that a platform or channel becomes vulnerable [20]. Information security risk is the harm to a process or the related information resulting from some purposeful or accidental event that negatively impacts the process or the related information. African banks consider regional expansion to be the key axis of their risk mitigation strategies [21]. However, lack of data regrettably did not allow assessing all risks and banks exposure is clearly increasing [22]. Financial crime usually involves fraud, but this can take many forms to exploit consumers, banks and government agencies. The most damaging seek to penetrate bank networks, with cybercriminals gaining access to accounts and siphoning money [23]. For this reason, information risks must be managed by understanding and responding to factors that may lead to a failure in the confidentiality, integrity or availability of an information system. Risk assessment process includes assessment of inherent risks and assessment of residual risks [24]. Inherent risk is the susceptibility of information or data to a material misstatement assuming that there are no mitigating control. It is a factor to be considered when determining the residual risk [25]. Residual risk is defined as the risk remaining after management takes action to reduce the severity and/or likelihood of an adverse event, including control activities in responding to a risk. Specifically, information system residual risk is the potential that a given threat will exploit a vulnerability of an asset and thereby cause harm whereas controls are in place. It is the risk remains even after all the security majors and controls to prevent risk are implemented [26]. In that context, safeguards and risk treatment allow to lower risk to a certain remaining value [27]. Residual criticality of risk represents the level of actual exposure and gives an appreciation of controls impact on inherent risks [28]. Practically, residual risks is obtained by estimating controls impact on inherent risks. However, in 2015, we propose a mathematical model which allow a quantification of banking residual risks [29]. After that, we also defined two mathematical models which provide an automatic calculation of internet banking controls maturity [30]. But the residual risk rating is often obtained by assessing the effect that the current controls have on inherent risk using the defined scales of risk likelihood and severity. To determine the residual risk rating, it is necessary to assess the effect that the control has on the overall risk leads [31]. As we can see, information system residual risks is estimated by assessors during several work sessions using a manual method which has some limits:

- it requires many work sessions with compromises in case of disagreement
- it requires significant level of expertise, time and personal investment
- the impact of implemented controls are differently appreciated by assessors
- they are some estimation error during assessment of residual risk

III. Contribution

In this paper, we automatize the residual risk estimation step of FMECA by proposing a new approach and defining a quantification model. FMECA is based on an inductive reasoning and study causes, effects of failures and criticality [32]. To propose our model, we consider the following 10 principles:

- Principle 1: A risk can have one or more controls which are set of measures to mitigate it
- Principle 2: A control is defined to reduce risk criticality which is an aggregated measure of risk
- Principle 3: Controls have one maturity and four types: deterrent, preventive, detective and corrective
- Principle 4: Deterrent Controls are intended to discourage a potential attacker
- Principle 5: Preventive controls are intended to minimize the likelihood of an incident occurring
- Principle 6: Detective controls are intended to identify when an incident has occurred
- Principle 7: Corrective controls are intended to fix information system components after an incident has occurred
- Principle 8: Only detected risks are corrected, when risks are not detected, corrective controls cannot be apply
- Principle 9: Only mature deterrent or preventive control can reduce risk likelihood
- Principle 10: Only mature detective or corrective control can reduce risk severity

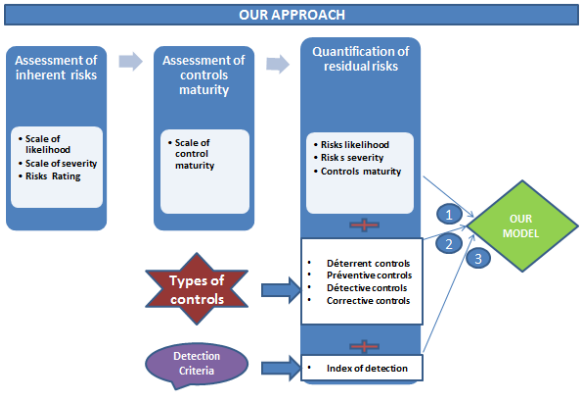

Figure 1. Our Model Approach

As illustrated above, we propose a quantification of security measures impact on banking information system risks using FMECA. The proposed approach has three steps and take into account controls maturity, types of controls and detection criteria. The first step concerns the assessment of inherent risks using the scales related to likelihood of occurrence and severity of impact in order to assign inherent value to each risk. The second step concerns assessment of control maturity using the scale of controls maturity in order to assign a maturity value to each control. The third step is related to quantification of residual values. This step take into account the parameters of the two previous step and additional parameters which are related to type of controls and detection criteria.

A. The defined scales

We defined different scales which will be model parameters. The used scales for likelihood and severity have six values at most; During inherent assessment, one value is assigned to risk likelihood and one value to risk severity. The following scale is defined to assess likelihood of the risk eventuating with no controls in place. This will inform the inherent risk rating and enable the effectiveness of any current controls that reduce the likelihood of a risk event occurring to be assessed.

Table I
VALUE OF RISK LIKELIHOOD

Rating	Description	Meaning
1	Almost Never	It is difficult for threats to exploit vulnerability
2	Unlikely	Threats require significant skills to exploit vulnerability
3	Possible	Threats require moderate skills to exploit vulnerability
4	Highly likely	Threats require minimal skills to exploit vulnerability
5	Almost Certain	It is easy for threats to exploit vulnerability
6	Very certain	It is very easy for threats to exploit vulnerability

The following scales is defined to assess the severity of the risk eventuating with no controls in place. This will inform the inherent risk rating and enable the effectiveness of any current controls that reduce the impact of a risk event that occurs to be assessed.

Table II
VALUE OF RISK SEVERITY

Rating	Description	Meaning
1	Minimal	Any impact on strategic objectives
2	Minor	Impact can be managed within current resources
3	Moderate	Impact can be managed with modest extra resources
4	Significant	Impact cannot be managed without extra resources
5	Severe	Impact cannot be managed without significant extra resources
6	Very severe	Could severely compromise strategic objectives

The used scale for controls maturity assessment is declined in the following table. As indicated, the scale has five values at most. Each assessed control will be assigned one value of maturity.

Table III
VALUE OF CONTROL MATURITY

Rating	Description	Meaning
1	Not Existent	Bank has not even identified the issues to be addressed.
2	Initial	Issues exist but the approach to management is disorganized.
3	Systematic	The procedures are not sophisticated but they are formalized
4	Managed	Management monitors and measures compliance with procedures
5	Optimized	Processes have been refined to a level of good practice

B. The defined index

We also define five index related to controls maturity and four types of controls which will be used on model equations. For each control maturity, we defined the corresponding index. As indicated below, the maturity index has tree values 0, 1 and 2.

Table IV
VALUE OF MATURITY INDEX

Rating	Index	Description
1	0	Not Existent
2	0	Initial
3	1	Systematic
4	2	Managed
5	2	Optimized

The following index is related to four types of controls. They have 2 values at most 0 or 1. We will also take account of this indexes when we calculated the impact of controls because every control has a value of maturity index and value of type index.

Table V
VALUES OF DETERRENT INDEX

Type of control	Index
Deterrent	1
Not deterrent	0

Table VI
VALUES OF PREVENTION INDEX

Type of control	Index
Preventive	1
Not preventive	0

Table VII
VALUES OF DETECTION INDEX

Type of control	index
Detective	1
Not detective	0

Table VIII
VALUES OF CORRECTIVE INDEX

Type of control	Index
Corrective	1
Not corrective	0

C. New proposed model

To define our model, we consider the previous principles, scales and indexes. We also take into account banking regulations, safety standards of information system and electronic payment, collaborations and partnerships. We also use the following definitions :

- Inherent risks: risk without consideration of controls
- Controls maturity : maturity of deterrent, preventive, detective and corrective controls
- Residual risks : risk after taking into account all types of controls

Considering the equation which provides risk criticality [33] by calculating the product of likelihood and severity, our model which automatize the assessment of security measures impact on banking information system risks is declined as follows:

$$C_{res} = [P-(\sum_{e=0}^{r}(a*i)/r+\sum_{e=0}^{s}(b*j)/s)]*[G-(\sum_{e=0}^{t}(c*k)/t+\sum_{e=0}^{u}((d/2)*l))/u)] \quad (1)$$

Our model parameters is explained below:

- Residual risks: Cres
- Inherent likelihood: P
- Inherent severity: G
- Equation(2) quantify the impact of deterrent controls using maturity of deterrent controls(a), index of deterrent controls(i) and number of deterrent controls(r). It is based on the principles 4 and 9 which says that deterrent controls are intended to discourage a potential attacker and when they are mature, they can reduce risk likelihood.

$$\sum_{e=0}^{r}(a*i)/r \quad (2)$$

- Equation(3) quantify the impact of preventive controls using maturity of preventive controls(b), index of preventive controls(j) and number of preventive controls(s). It is based on the principles 5 and 9 which says that preventive controls are intended to minimize the likelihood of an incident occurring and when they are mature, they can reduce risk likelihood.

$$\sum_{e=0}^{s}(b*j)/s \quad (3)$$

- Equation(4) quantify the Impact of detective controls using maturity of detective controls(c), index of detective controls(k) and number of detective controls(t). It is based on the principles 6 and 10 which says that detective controls are intended to identify when an incident has occurred and when they are mature, they can reduce risk severity.

$$\sum_{e=0}^{t}(c*k)/t \quad (4)$$

- Equation(5) quantify the impact of corrective controls using maturity of corrective controls(d), index of corrective controls(l) and number of corrective controls(u). It is based on the principles 7 and 10 which says that corrective controls are intended to fix information system components after an incident has occurred and when they are mature, they can reduce risk severity. Principle 8 is also used because only detected risks are corrected, that means when risks are not detected, corrective controls cannot be apply. As told before, we know that the maximum of index maturity is 2; then we propose that maturity of deterrent, preventive and detective controls does not need to be modify because they are independent. But maturity of corrective controls must be divided by 2 because they depend to control detection.

$$\sum_{l=0}^{e}((d/2)*l))/u \quad (5)$$

IV. TESTS AND RESULTS

For testing, we collaborated with banks which offer traditional banking services and electronic banking products like withdrawal, payment or transfer using credit, debit or prepaid cards. This sample is representative because other banks have approximately the same risks considering their similar activity, infrastructure and their dependance to laws and regulations. For reasons of confidentiality, we will not disclose identity of those banks.

A. Risks identification

To identify information system risks, it is necessary to take account threats and vulnerabilities because the concerned risk is defined as the exercise of a threat against a vulnerability. Threats identification includes threat-sources to ensure accurate assessment and vulnerabilities can be identified by numerous means. After identification sessions, we have collected 106 risks and 205 controls related to banking information system.

B. Inherent risks assessment

Assessing inherent risks is the process of determining the likelihood of the threat being exercised against the vulnerability and the resulting impact from a successful compromise. When assessing inherent likelihood and severity, we do not take into consideration the implemented controls. During assessment, we assigned to each risks a value of likelihood and severity using the previous defined scale

C. Residual risks assessment

Residual risk assessment estimates likelihood of threats which are not avoided by security measures, such as residual threats. Those threats can be eliminated by additional security measures. In this way, risk will be reduced to an acceptable level [34]. After the evaluation of the identified risks and controls, risks were reassessed during the working sessions with the concerned assessors in order to obtain an estimate of residual risks. The inherent risks combined with controls assessment provide residual risks which are called reference values.

D. Application of the model on all information system risks

For testing, we apply the model on all banking information system risks and compare the obtained values to values given by assessors which are called references values. Before approving the model, we test it on information system components, information security criteria and SDLC (Software Development Life Cycle) phases.

1) Application of the model on information system components: We classify all risks by information system components which include hardware, software, network, data base, site, information and users before applying the model. For this we calculate for each component, the average of control maturity by type of controls, identified the number of controls and apply the proposed model. The correlation rate between model and reference residual risks is shown in the following table . We remarked that correlation rate by component is between 95.8% and 97.8%. That means for each information system component, model values are approximately equal to reference values. Correlation rate average is equal 97%, that means that the residual risks by information system component is globally equal to reference values given by assessors.

We also design the graph related to model and reference residual risks. We can see that model values are equal, upper or lower than reference values as indicated in the following graph. That means residual values between model and reference by information system component are random .

Table IX
CORRELATION RATE BETWEEN MODEL AND REFERENCE RESIDUAL RISKS BY INFORMATION SYSTEM COMPONENTS

Information System Components	Correlation Rate
Hardware	96.6%
Software	97.5%
Network	97.8%
Data base	96.7%
Site	97.3%
Information	95.8%
Users	96.8%
AVERAGE	97%

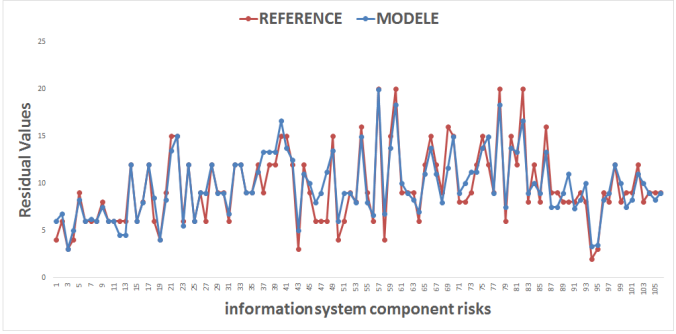

Figure 2. Residual Values by information system component risks

2) Application of the model on information security criterias: We also classify all risks by information security criterias which include effectiveness, efficiency, integrity, confidentiality, compliance, availability, reliability before applying the model. For this we calculate for each criteria, the average of control maturity by type of controls, identified the number of controls and apply the proposed model. The correlation rate between model and reference residual risks is shown in the following table:

Table X
CORRELATION RATE BETWEEN MODEL AND REFERENCE RESIDUAL RISKS BY INFORMATION SECURITY CRITERIA

Information Security Criteria	Correlation Rate
Effectiveness	97%
Efficiency	97.3%
Integrity	96.8%
Confidentiality	97%
Compliance	96.9%
Availability	97.3%
Reliability	96.1%
AVERAGE	97%

We remarked that correlation rate by concerned criteria is different and its value is between 96.1% and 97.3%. That means for each criteria, model values are approximately equal to reference values. Correlation rate average is the same because the tests are done on all information system and its value 97% shows that model values are globally equal to reference values.

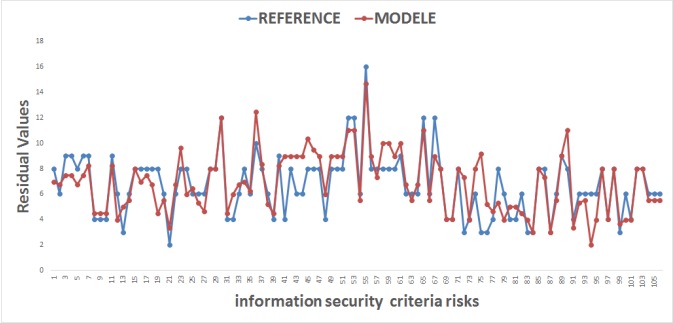

Figure 3. Residual Values by information security criteria risks

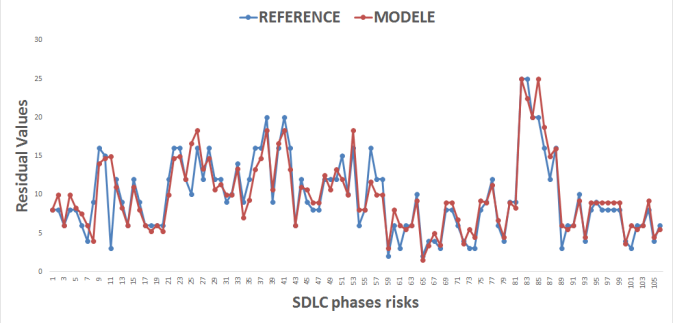

Figure 4. Residual Values by SDLC phases risks

As indicated in the graph above, we can see that model values are equal, upper or lower than reference values. That means residual values between model and reference by information security criteria are random.

3) Application of the model on SDLC phases: We finally classify all risks by SDLC (Software Development Life Cycle) phases. Those phases include seven different steps: requirement, analysis, design, development, test and maintenance [35]. For testing, we calculate for each phase, the average of control maturity by type of controls, identified the number of controls and apply the proposed model. The correlation rate between model and reference residuals risks is shown in the following table:

Table XI
CORRELATION RATE BETWEEN MODEL AND REFERENCE RESIDUAL RISKS BY SDLC PHASES

SDLC Phases	Correlation Rate
Requirement	96.8%
Analysis	96,7%
Design	97.6%
Development	96.7%
Test	97.5%
Maintenance	96.8%
AVERAGE	97%

We remarked that correlation rate value by SDLC phases is different and its value is between 96.7% and 97.6%. That means for each SDLC phases, model values are approximately equal to reference values .Correlation rate average is always the same because the tests are done on all identified risks and its value which is equal to 97% shows that the model residual risks are globally equal to reference residual risks. In order to appreciate the difference, we design the graph which showed model and reference residual risks. As we can see, model values are equal, upper or lower than reference values. That means residual values between model and reference by SDLC phases are random. the concerned graph is declined as follow:

E. Gain of time

Finally, we measure the gain of time provided by our model as indicated in the table below:

Table XII
GAIN OF TIME PROVIDED BY OUR MODEL

Criteria	Gain of time for 1 Assessor	Gain of time for 10 Assessors
per risk	30 minutes	5 hours
per 20 risks	1.25 man-days	12.5 man-days
per 40 risks	2.5 man-days	25 man-days
per 60 risks	3.75 man-days	37.5 man-days
per 80 risks	5 man-days	50 man-days
per 100 risks	6.25 man-days	62.5 man-days

As we can see in the table above, our model provides a win of time of 62.5 man-days for assessment of 100 information system risks by 10 assessors. This may be very beneficial for banks because we know that the different assessors have many tasks to be carried out in their respective departments. Our model helps to avoid wasting considerable time during residual risks assessment.

F. Global Results

Considering, the good correlation rate between model and reference residual risks and the win of time provided by the model, we conclude that our model has several advantages which are listed below:

- Automatic calculation of information system residual risks considering the good correlation rate between model values and reference values
- Decrease of residual risks estimation error by harmonizing assessment methods and scales
- Reduction of time for obtaining residual risks considering the gain of time provided by the model
- Help on improvement of banking information system security by automatizing assessment of security measures maturity
- Facilitation of risks management by automatizing risks and controls assessment

V. Conclusion

Banking information system is very exposed to cybercrime and others attacks. For this reason, assessment of security measures maturity must be optimal in order to implement appropriate controls whenever it is necessary. In this paper, we define a mathematical model which quantify the impact of security measures on banking information system risks and we obtain a good correlation rate between model and reference residuals risks. Test Results are satisfactory by information system components, information security criterias and software development life cycle phases. The model provides automatic calculation of residual risks, decrease estimation error rate and reduce time for obtaining residual risks. This implies improvement of banking information system security, facilitation of risk management and increase of bank profit. In our future work, we will try to improve the model by increasing correlation rate, reduce parameters of the equation and extend tests to operational and compliance risks.

Acknowledgment

The authors would like to thank to Mr Ibrahima Gaye for his contribution on model testing.

References

[1] "Risk Management and Accreditation of Information Systems," National Infrastructure Security, August 2005

[2] G. Stoneburner, A. Goguen and A. Feringa, "Risk Management Guide for Information Technology Systems," National Institure of Standars and Technology, Sweden, Special Publication 800-30, July 2002

[3] "Risk Assessment and Risk Management Methods: Information Packages for Small and Medium Sized Enterprises (SMEs)," ENISA ad hoc working group on risk assessment and risk management: Deliverable 2, Final version, March 2006

[4] K. Kohout, "IT Risk Register, faculty of informatics and statistics," Prague, December 2012

[5] G. Hardy and J. Heschl, "Aligning CobiT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit," IT Governance Institute, 2008

[6] A. Syalim, Y. Hori and K. Sakurai, "Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsofts Security Management Guide," Kyushu University, Fukuoka, Japan

[7] V. Arora, "Comparing different information security standards: COBIT v s. ISO 27001," Carnegie Mellon University, Qatar

[8] M. Gehrmann, "Combining ITIL, COBIT and ISO/IEC 27002 for structuring comprehensive information technology for management in organizations," Navus Revista de Gesto e Tecnologia. Florianpolis: ISSN 2237-4558, Aout 2012

[9] I. Mukherjee, "Cloud Security Through COBIT, ISO 27001 ISMS CONTROLS, ASSURANCE AND COMPLIANCE," ISACA, RSA Conference ASIA PACIFIC, Singapore, 2013

[10] "Organisation Resilience: Business Continuity, Incident and Corporate Crisis Management," Institute of Business Continuity Management, NPC 2012

[11] C. Periou, "New players and new banking models for Africa," May 2013

[12] "Payments 101: Credit and Debit Card Payments," Key Concepts and Industry Issues, A First Data White Paper, October 2010

[13] P. Dulany, H. Gong and K. Shah, "CA Technologies, Advanced Analytics and Data Science: 3D-Secure Authentication using Advanced Models," White paper, October 2014

[14] "Card-Not-Present Fraud Working Committee White Paper," Near-Term Solutions to Address the Growing Threat of Card-Not-Present Fraud, Biometrics in Banking and Payments, Javelin Strategy Research, www.javelinstrategy.com, April 2015

[15] R. Anderson, "Risk and Privacy Implications of Consumer Payment Innovation," Cambridge University

[16] "Review of the Risk Assessment Process for Payment Systems," Risk Assessment Review, May 2013

[17] J. Conroy, "3D Secure: The Force for CNP Fraud Prevention Awakens," january 2016

[18] P. Kellogg, "Evolving Operational Risk Management for Retail Payments," Federal Reserve bank of Chicago, Emerging Payments Occasional Papers Series, 2003

[19] A. L. Pereira and A. M. de Alba, "Understanding the new payment methods, their risks and opportunities," LexisNexis, Risk Solutions, 2011

[20] P. Burns and A. Stanley, "Fraud Management in the Credit Card Industry," 1st ed Discussion paper, Payment Card Center, Federal Reserve Bank of Philadelphia, April 2002

[21] C. Periou, "New players and new banking models for Africa," May 2013

[22] W. S. Koffi, "The Fintech Revolution: An Opportunity for the West African Financial Sector," School of Economics, 2016

[23] "Net Losses: Estimating the Global Cost of Cybercrime," Economic impact of cybercrime II, June 2014

[24] D. Weese, "Overview of risk assessment methods and applications," Executive Director of AMGEC, June 2006

[25] A. Ho, "Integration and use of Enterprise Risk Management (ERM) information," Enterprise Risk Management Symposium, Chicago, April 22-23 2013

[26] N. Mathur, H. Mathur and T. Pandya, "Risk Management in Information System of Organisation: A Conceptual Framework," International Journal of Novel Research in Computer Science and Software Engineering Vol. 2, Issue 1, pp: (82-88), Month: January-April 2015

[27] O. Pastor, L. J. G. Villalba and D. Lpez, "DYNAMIC RISK ASSESSMENT IN INFORMATION SYSTEMS: STATE-OF-THE-ART," The 6th International Conference on Information Technology, ICIT 2013

[28] B. Jenkins, "Risk Analysis helps establish a good security posture; Risk Management keeps it that way," Countermeasures.Inc, 1998

[29] M. Ndaw, G. Mendy and S. Ouya, "A quantification model of internal control impact on banking risks using FMECA," IEEE 5th World Congress on Information and Communication Technologies (WICT), Marakech, 2015

[30] M. Ndaw, G. Mendy and S. Ouya, "Quantify the Maturity of Internet Banking Security Measures in WAEMU (West African Economic and Monetary Union) Banks," EAI International Conference on Innovations and Interdisciplinary Solutions for Underserved Areas, APRIL 2017, Dakar, Senegal

[31] "Risk Assessment Process Information Security," All-of-Government Risk Assessment Process: Information Security, February 2014

[32] L. Lipol and J. Haq, "Risk Analysis Method: FMEA/FMECA in the Organizations," University of Boras, Sweden: IJBAS-IJENS Vol: 11 No: 05, 2011

[33] V. Dumbrav, T. Maiorescu and V. S. Iacob, "Using Probability Impact Matrix in Analysis and Risk Assessment," Projects Scientific Papers (www.scientificpapers.org), Journal of Knowledge Management, Economics and Information Technology, Special Issue, December 2013

[34] B. Nikoli and L. R. Dimitrijevi, "Risk Assessment of Information Technology Systems," The Higher Education Technical School of Professional Studies, Novi Sad, Serbia, Issues in Informing Science and Information Technology Volume 6, 2009

[35] K. Sahu, Rajshree and R. Kumar, "Risk Management Perspective in SDLC," Kavita et al., International Journal of Advanced Research in Computer Science and Software Engineering 4 (3), March-2014, pp. 1247-1251, 2014