World Academy of Science, Engineering and Technology
International Journal of Economics and Management Engineering
Vol:10, No:2, 2016

Modeling the Impact of Controls on Information System Risks

M. Ndaw, G. Mendy, S. Ouya

Abstract—Information system risk management helps to reduce or eliminate risk by implementing appropriate controls. In this paper, we propose a quantification model of controls impact on information system risks by automatizing the residual criticality estimation step of FMECA which is based on a inductive reasoning. For this, we defined three equations based on type and maturity of controls. For testing, the values obtained with the model were compared to estimated values given by interlocutors during different working sessions and the result is satisfactory. This model allows an optimal assessment of controls maturity and facilitates risk analysis of information system.

Keywords—Information System, Risk, Control, FMECA.

I. Introduction

INFORMATION SYSTEM risk management helps to identify, control and mitigate concerned risks. It includes risk assessment, cost-benefit analysis and selection, implementation, test and evaluation of safeguards. A threat is a potential for a particular threat-source to successfully exercise a particular vulnerability and vulnerability is a weakness that can be accidentally triggered or intentionally exploited [1]. Risk is a function of the likelihood of a given threat-source's and the resulting impact of that adverse event on the organization [2]. In that context, implementation of best practices should be consistent with the enterprise's risk management and control framework, appropriate for the enterprise, and integrated with other methods and practices that are being used[3]. To manage risks which have major business impacts for the company, it is necessary to inhibit threat, reduce and eliminate vulnerability, protect and move asset [4]. Information security risk management process can be split into three activities [5]:

- Risk identification: Identification of assets, threats, vulnerabilities and consequences
- Risk analysis: Assessment of consequences, incident likelihood and level of risk determination
- Risk evaluation: Finalize a list of risks prioritized according to risk evaluation criteria in relation with incident scenarios that lead to those risks

Several information security standards like ITIL, COBIT, ISO 27001 and MEHARI are defined:

- ITIL is a library of good practices related to the services of information technology and provides a framework for good practices to guide the management of IT services [6].
- COBIT is a high-level IT governance and a framework of best practices in managing resources, infrastructure, processes, responsibilities and controls [7].
- ISO 27001 defines methods and practices of implementing information security in organizations with detailed steps on how they are implemented [8].
- MEHARI is a method for risk analysis and risk management which aims to provide a set of tools specifically designed for security management [9].

These standards are compared below:

TABLE I
Comparison between Standards

Standards	Approach	Utility
ITIL	Process	Management of IT services
COBIT	Process	Governance of IT services
MEHARI	Risk	Analyze and handle computing risks
ISO27001	Control	Management of the security

Security controls are also proposed and can be grouped into different families: [10]

- Access Control and Use Limitation
- Awareness and Training
- Audit and Accountability
- Security Assessment and Authorization
- Configuration Management
- Contingency and Planning
- Identification and Authentication
- Incident Response and Media Protection
- Maintenance and Planning
- Physical and Environmental Protection
- Personnel Security
- Risk Assessment
- System and Services Acquisition
- System and Communications Protection
- System and Information Integrity
- Program Management
- Authority and Purpose
- Accountability and Audit
- Data Quality and Integrity
- Data Minimization and Retention
- Individual Participation and Redress
- Security and Transparency

Information system risk management helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process.

M. Ndaw is a PHD Candidate at ESP (Ecole Superieur Polytechnique), UCAD (Universite Cheikh Anta DIOP), Dakar, Senegal (e-mail: lisandaw@gmail.com).

G. Mendy and S. Ouya are Teachers at ESP (Ecole Superieur Polytechnique), UCAD (Universite Cheikh Anta DIOP), Dakar, Senegal (e-mail: gervais.mendy@ucad.edu.sn, samuel.ouya@ucad.edu.sn

II. Related Works

Several methods exist for risk assessment [11]. The used method FMECA [12] is based on an inductive reasoning to study causes, effects of failures and their criticality. We choose this method because it is most detailed, scalable and practical to examine high or small level systems. Residual criticality of risk represents the level of actual exposure [13] and gives an appreciation of the impact of controls on risk criticality. It is obtained by estimation of residuals likelihood and severity during work sessions using FMECA method. This step of FMECA method has some limits:

- requires many work sessions with compromises in case of disagreement
- requires significant level of expertise
- requires time and personal investment
- the impact of internal control are appreciated differently by interlocutors
- they are some estimation error rate of residual risk criticality

III. Our Contribution

In our work, we propose automatic calculation of residual criticality of information system risk based on control maturity and type using FMECA Method. Such a model has several advantages including:

- Automatize calculation of risks residual criticality
- Decrease estimation error rate of residual criticality
- Reduce time for obtaining residual criticality
- Optimize assessment of controls maturity
- Facilitate risk management of information system

A. Model Principles

To propose this model, we used the following 7 principles:

- Principle 1: Risk may have one or more controls
- Principle 2: Control is defined to treat the identified and assessed risks
- Principle 3: Control has one maturity and three types
- Principle 4: Only mature control can reduce likelihood and severity of risk
- Principle 5: Preventive control may reduce likelihood of the risk (P)
- Principle 6: Detective control may reduce severity of the risk (G)
- Principle 7: Corrective control may reduce severity of the risk (G)

B. The Proposed Model

The proposed model is declined as follows:

$$C_{resu} = [P_{ini} - \sum_{1}^{ni}(a_i * i)] * G_{ini} - [(\sum_{1}^{nj}(a_j * j)) + (\sum_{1}^{nk}(a_k * k))] \quad (1)$$

The proposed model has six independent parameters:

- $[a_i] : MaturityIndexofpreventivecontrols$
- $[a_j] : MaturityIndexofdetectivecontrols$
- $[a_k] : MaturityIndexofcorrectivecontrols$
- $[i] : Preventionindex$
- $[j] : Detectionindex$
- $[k] : Correctionindex$

And depends on 5 independent variables:

- $[ni] : numberofpreventivecontrols$
- $[nj] : numberofdetectivecontrols$
- $[nk] : numberofcorrectivecontrols$
- $[P_{ini}] : inherentlikelihoodofrisk$
- $[G_{ini}] : inherentseverityofrisk$

IV. Test Data

A. Identification of Risks and Controls

We identify risks and controls by analyzing banking information system and taking into account collaborations and partnerships. Each identified risk has wording, cause, consequence, specific code and 3 controls at most. After identification sessions, we have collected 80 risks and 119 controls as indicated in the table:

TABLE II
Number of Identified Risks and Controls

Components	Risks Number	Controls Number
Hardware	13	20
Software	12	15
Network	13	17
Data base	10	18
Application	7	11
Information	10	13
Users	15	25
TOTAL	80	119

B. Evaluation of Risks and Controls by Interlocutors

We quantified each identified risk and assigned it likelihood, severity and criticality using the following scales of likelihood and severity:

TABLE III
Value of Likelihood

Value	Signification
1	Very unlikely
2	Unlikely
3	Likely
4	Very likely
5	Certain
6	Very certain

TABLE IV
Value of Severity

Value	Signification
1	Insignificant
2	Not serious
3	Severe
4	Very severe
5	Crisis
6	Major crisis

A control has three types (preventive, detective or corrective) and one maturity according to the following scale:

C. Estimates of the Residual Criticality Risk by Interlocutors

After the evaluation of identified risks and controls, inherent likelihood and severity of risk were reassessed during the working sessions with the concerned interlocutors in order to

TABLE V
VALUE OF CONTROL MATURITY

Value	Signification
1	Not Present
2	Informal
3	Systematic
4	Integrated
5	Optimized

obtain an estimate of the residual criticality of each risk. The inherent risk assessment combined with the assessment of the controls maturity and type will give the level of residual risk which is the actual level of exposure. The result of inherent and residual assessment is illustrated in the following table:

TABLE VI
AVERAGE OF INHERENT AND RESIDUAL CRITICALITY

IS Component	Inherent Criticality	Residual Criticality
Hardware	9.70	8.30
Software	16.20	10.13
Network	11.36	8.34
Data base	14.15	10.13
Application	13.35	10.12
Information	14.70	9.93
Users	10.51	9.42
TOTAL	12.85	9.48

V. TESTS

A. Application of the Model on Information System Component

We test the model on 80 risks and 119 controls, calculate for each risk the average of control maturity and identified the number of controls. The comparison between model and estimation is shown in the following table:

TABLE VII
ESTIMATION VS MODEL BY INFORMATION SYSTEM COMPONENT

IS Compnt	EstimValues	ModelValues	ResidValues	CorrelRate
Hardware	8.30	8.56	0.25	97%
Software	10.13	10.05	-0.08	99%
Network	8.34	8.55	0.21	98%
Data base	10.13	10.55	0.42	96%
Application	10.12	9.96	-0.16	98%
Information	9.93	10.37	0.43	96%
Users	9.42	9.73	0.31	97%
TOTAL	9.48	9.68	0.2	98%

The following graphs compare the model and estimation.

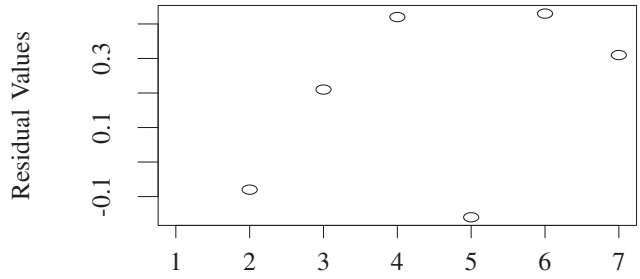

Fig. 1 Average by IS component risks
Our Model vs Estimation

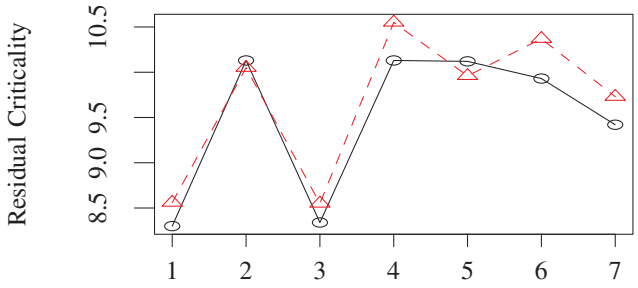

Fig. 2 Average by IS component risks
Our Model(red) vs Estimation(black)

VI. RESULTS 1

- Correlation rate by information system component is equal 98%
- Residual values between model and estimation by information system component are random

A. Application of the Model on Information Criteria

After that, we test the model on 7 information criteria [15]. The comparison between model and estimation is shown in the following table:

TABLE VIII
ESTIMATION VS MODEL BY INFORMATION CRITERIA

Info Criteria	EstimValues	ModelValues	ResidValues	CorrelRate
Effectiveness	9.30	9.20	-0.10	99%
Efficiency	11.13	11.05	-0.08	99%
Integrity	8.34	8.20	0.21	98%
Confidentiality	10.13	10.75	0.62	94%
Compliance	8.12	8.36	0.24	97%
Availability	10.93	11.20	0.27	98%
Reliability	8.42	9.00	0.58	94%
TOTAL	9.48	9.68	0.2	98%

The following graphs compare the model and estimation:

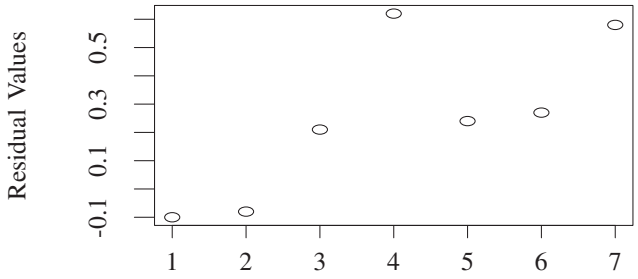

Fig. 3 Average by information criteria risks
Our Model vs Estimation

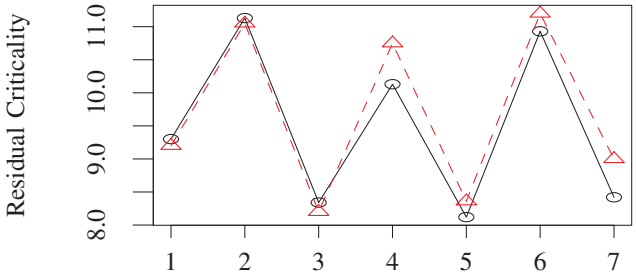

Fig. 4 Average by information criteria risks
Our Model(red) vs Estimation(black)

VII. Results 2

- Correlation rate by information criteria is equal 98%
- Residual values between model and estimation by information criteria are random

A. Application of the Model on SLDC Phases

We also test the model on SDLC(System Development Life Cycle) phases [1] as shown in the following table.

TABLE IX
Estimation vs Model by SDLC Phases

SDLC Phases	EstimVal	ModelVal	ResidVal	CorrelRate
Initiation	8.66	8.98	0.22	98%
Acqtion/Devpt	8.13	8.33	0.20	98%
Implementation	10.53	10.45	-0.08	99%
Operation	9.34	9.96	0.22	98%
Disposal	10.73	10.67	-0.07	99%
TOTAL	9.48	9.68	0.01	98%

The following graphs compare the model and estimation:

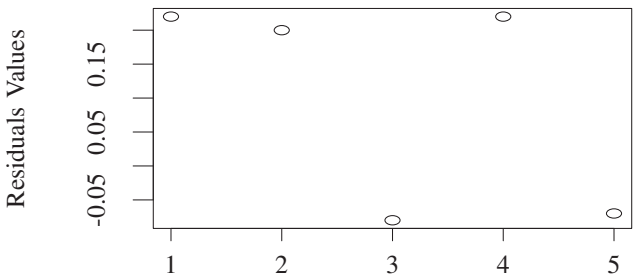

Fig. 5 Average by SDLC phases risks
Our Model vs Estimation

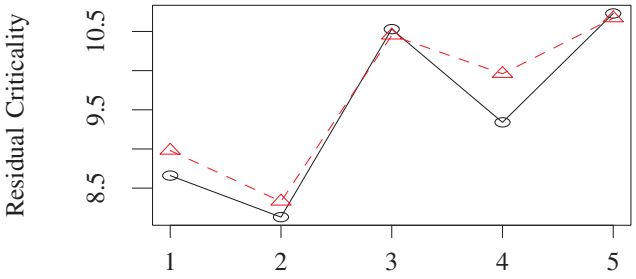

Fig. 6 Average by SDLC phases risks
Our Model(red) vs Estimation(black)

VIII. Results 3

- Correlation rate by SLDC phases is equal 98%
- Residual values between model and estimation by SLDC phases are random

A. Application of the Model on Risk Sources

We finally test the model on risk sources as shown in the following table:

TABLE X
Estimation vs Model by Risk Sources

Risk Sources	EstimVal	ModelVal	ResidVal	CorrelRate
Environment	10.26	9.90	0.22	98%
Partnership	8.13	8.40	0.27	97%
Compliance	10.11	9.95	-0.16	98%
Int/Ext Fraud	8.31	9.66	0.22	98%
Logi/Phys Acces	10.60	10.51	-0.10	99%
TOTAL	9.48	9.68	0.01	98%

The following graphs compare the model and estimation:

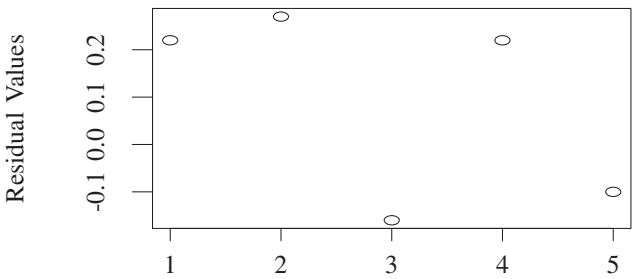

Fig. 7 Average by risk sources
Our Model vs Estimation

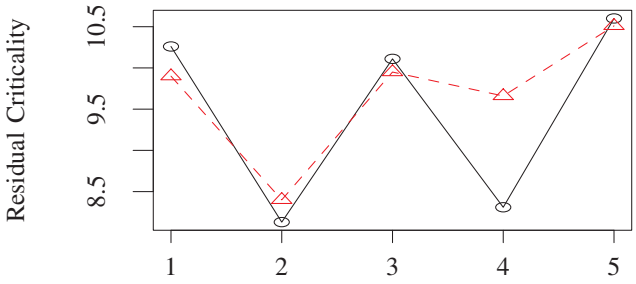

Fig. 8 Average by risk sources
Our Model(red) vs Estimation(black)

IX. Results 4

- Correlation rate by risk sources is equal 98%
- Residual values between model and estimation by risk sources are random

X. Conclusion

In this paper, we defined a mathematical model which quantify the impact of controls on information system risks. This model does not require evaluation sessions, decreases estimation error and makes automatic risk residual criticality estimation step of FMECA Method. After testing, the correlation rate between estimation and model is around 98%. Our future works could be summarized as follows:

- Improve the model by increasing correlation rate
- Reduce parameters and variables of proposed equations
- Increase controls and size of likelihood and severity scale
- Extend tests to others banking process
- Use another method different to FMECA

Appendix A
Proof of the First Equation

Equation (1) is based on the principles 1, 2, 3, 4 and 5 and provides residual likelihood of risk. For this, we defined two indexes (a: maturity index and i: prevention index)

TABLE XI
Values of Maturity Index

Value	Meaning	Index
1	not present	0
2	Informal	0
3	Systematic	1
4	Integrated	1
5	Optimized	2

TABLE XII
Values of Prevention Index

Type of control	Index
Preventive	1
Not preventive	0

Considering these indexes, the residual likelihood is defined as follows:

- Residual likelihood = inherent likelihood - maturity of preventive controls

$$P_{resu} = P_{ini} - \sum_{1}^{ni}(a_i * i) \quad (2)$$

$[a_i] : 0, 1, 2/i : 0, 1/ni : 1, 2, 3$

Appendix B
Proof of the Second Equation

Equation (2) is based on the principles 1, 2, 3, 4, 6 and 7 and provides the residual severity of risk. For this, we used a: maturity index defined above and added two additional indexes (j: detection index and k: correction Index)

TABLE XIII
Values of Detection Index

Type of control	index
Detective	1
Not detective	0

TABLE XIV
Values of Corrective Index

Type of control &Index	
Corrective &1	
Not corrective &0	

- Residual severity = inherent severity - maturity of detective and corrective controls

$$G_{resu} = G_{ini} - [(\sum_{1}^{nj}(a_j * j)) + (\sum_{1}^{nk}(a_k * k))] \quad (3)$$

$[a_j, a_k] : 0, 1, 2/[j, k] : 0, 1/[nj, nk] : 1, 2, 3$

Appendix C
Proof of the Third Equation

Equation (3) is based on the existing equation of criticality (C) [14] which is the product of likelihood of occurence (P) and severity of harm (G). Residual criticality is the product of (1) and (2):

- Equation (3) = Equation (1) * Equation (2)
- Residual criticality = Residual likelihood * Residual Severity

$$C_{resu} = [P_{ini} - \sum_{1}^{ni}(a_i * i)] * [G_{ini} - [(\sum_{1}^{nj}(a_j * j)) + (\sum_{1}^{nk}(a_k * k))] \quad (4)$$

$[a_i, a_j, a_k] : 0, 1, 2/[i, j, k] : 0, 1/[ni, nj, nk] : 1, 2, 3$

APPENDIX D
GLOSSARY

- IT: Information Technology
- IS: Information System
- IT Risk: Net mission impact considering the probability that a particular threat-source will exercise a particular information system vulnerability and the resulting impact if this should occur
- Risk Assessment: Process of identifying the risks to system security and determining the probability of occurrence, the resulting impact and additional safeguards that would mitigate this impact
- Risk Management: Total process of identifying, controlling and mitigating information systemrelated risks.This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations and laws
- Information system security: System characteristic and a set of mechanisms that span the system both logically and physically
- Risk exposure: Variable to measure risks which organization is actually exposed
- Likelihood of risk: Possibility for a risk to occur
- Severity of risk: Negative consequences of risk
- Control: Set of measures to control risks
- Preventive control: Based on preventing the risk occurring
- Detective control: Based on risk communication out
- Corrective control: Based on treatment of risk detected
- Criticality: Aggregated measure of risk
- Inherent criticality: Criticality without consideration of controls
- Residual criticality: Criticality after taking into account the controls
- FMECA Method: Failure Modes and Effect Criticality Analysis Method

REFERENCES

[1] G. Stoneburner, A. Goguen, and A. Feringa, Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology, Sweden: Special Publication 800-30, July 2002.
[2] Risk Management and Accreditation of Information Systems, National Infrastructure Security, August 2005.
[3] G. Hardy, J. Heschl, Aligning CobiT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit, IT Governance Institute, 2008.
[4] Risk Assessment and Risk Management Methods: Information Packages for Small and Medium Sized Enterprises (SMEs), ENISA adhoc working group on risk assessment and risk management: Deliverable 2, Final version, March 2006.
[5] K. Kohout, IT Risk Register, Faculty of informatics and statistics, Prague, December 2012.
[6] 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, August 2012.
[7] I. Mukherjee, Cloud Security through COBIT, ISO 27001 ISMS Controls, Assurance and Compliance, ISACA, RSA Conference ASIA PACIFIC, Singapore, 2013.
[8] V. Arora, Comparing different information security standards: COBIT v s. ISO 27001, Carnegie Mellon University, Qatar.
[9] A. Syalim,Y. Hori and K. Sakurai, Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide, Kyushu University, Fukuoka, Japan.
[10] CMS Information Security Acceptable Risk Safeguards (ARS), CMS Minimum Security Requirements (CMSR), Enterprise Information Security Group, Baltimore, Maryland: FINAL Version 2.0, September 20, 2013.
[11] Residual Risk Assessment for the Pulp & Paper, EPAs Office of Air Quality Planning and Standards Office of Air and Radiation, December 2011.
[12] L. Lipol and J. Haq, Risk Analysis Method: FMEA/FMECA in the Organizations, University of Boras, Sweden:IJBAS-IJENS Vol: 11 No:05, 2011.
[13] G. Tolbert, Residual Risk Reduction, Georgia, November 2005.
[14] B. Jenkins, Risk Analysis helps establish a good security posture; Risk Management keeps it that way, Countermeasures Inc., 1998.
[15] L. Lipol, J. Haq, COBIT Mapping: Mapping of ITIL V3 with COBIT 4.1, IT Governance Institute, USA: ISBN 978-1-60420-035-5, 2008.

Marie Ndaw: holds Bachelor degree on Mathematics and Computer Science and Master's degree on IT security at Rabat faculty of Sciences, Mohammed V University, Morocco. She has 7 years of experience in Banking as software engineer, project manager and she is responsible for electronic Banking exploitation. Presently, she is Senior Internal Auditor at Electronic Banking Group of West African Economic and Monetary Union and PHD candidate at ESP (Ecole Superieur Polytechnique), Cheikh Anta DIOP University, Dakar, Senegal.

Gervais Mendy: has a PHD on Network and Computer Science, Dorsey University, South of Paris. The author is a teacher at ESP (Ecole Superieur Polytechnique) and the Head of Software Engineering Department at Cheikh Anta DIOP University Dakar, Senegal.

Samuel Ouya: has a PHD on Applied mathematics and Digital analysis. The author is a teacher at Polytechnic High School and the Head of LIRT (laboratoire Informatique Reseaux et Telecoms) at Cheikh Anta DIOP University Dakar, Senegal.