International Journal of Computer Science and Business Informatics

IJCSBI.ORG

Cost Estimation of Information Technology Risks and Instituting Appropriate Controls

Princewill Aigbe
Department of Mathematics and Computer Science
Western Delta University
Oghara Delta State
Nigeria

Jackson Akpojaro
Department of Mathematics and Computer Science
Western Delta University
Oghara Delta State
Nigeria

ABSTRACT
Nothing puzzles an enterprise's Information Technology (IT) manager like the term "cost value" when deciding investments made in IT risk management. Therefore, a detailed analysis of data-driven approach in managing IT risks and reducing or eliminating disproportionate expenditure on controls is given. This paper is structured in two major sections: the risk analysis stage, where IT risks are identified and estimated, and the control selection stage, where the cost of appropriate control is selected to reduce or eliminate a given IT risk. The paper works through a selected case study scenario to practically demonstrate the data-driven approach.

Keywords
Information technology risk, data-driven techniques, enterprise risk management, expenditure.

1. INTRODUCTION
There are many definitions of risk, reflecting that risk means different things to different people. The International Organization for Standardization (ISO) definition is that, risk is the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. This definition is used commonly by the industry since it puts risk into an organizational context by using the concepts of assets and loss of value – terms that are easily understood by business managers.

Risk is also defined as the possibility of damage or loss [1]. The word risk denotes that a decision maker knows the possible consequences of a decision and its relative likelihood at the time the decision was made. The

ultimate decisions to be made in IT investments are: estimates are prepared of the risk and return over the investment holding period (investment analysis) and risk-return estimates are compared to decide how to allocate available funds among these investments on a continuing basis (IT portfolio analysis, selection and management).

In the process of estimating IT risk, the identification of risks and vulnerabilities, and also understanding the relationship between risk and control is very important in order to determine the necessary controls needed to reduce these risks. In the Certified Information Systems Auditor (CISA) study guide [13], controls are policies, procedures, practices and organizational structures implemented to reduce identified risks. There are two key aspects that controls should address: these are what should be achieved, and what should be avoided. In addition, not only do controls address operational objectives, but they should also address undesired events through prevention, detection and correction.

Organizations whose business processes are heavily IT dependent are threaten with a number of information technologies related risks. These risks must be carefully identified, classified, and analyzed for the purpose of estimating their costs. In the process of estimating the cost of a given risk, some determinants are adopted in the risk analysis stage. These determinants are risk probability, average restoration cost, and cost at risk. It is when the cost of a given identified risk has been estimated, that appropriate control can be instituted to reduce (or eliminate) such risk. In arriving at the best control to reduce an identified IT risk, there are also determinants that must be procedurally followed in the control selection stage. These determinants are residual risk, control lost, cost at risk (with control), cost of control, and cost-value proposition.

The remaining part of the paper is structured as follows; in Section 2, we discuss the methodological approaches for analyzing and evaluating risks. Section 3 specifies the organization we use as case study and method of data collection. In Section 4, we analyze and discuss our research findings. Section 5 concludes the work.

2. METHODOLOGY

The estimation of the cost of a given IT risk and the selection of appropriate control(s) to reduce the risk, using the various determinants highlighted above is a two-stage process, which involves risk analysis and evaluation of risk probability.

2.1 Risk Analysis

Risk analysis includes the following steps: Explore threats and Vulnerabilities. These steps explore the threats and vulnerabilities of the systems, spread across the investigation scope, through a thorough analysis of the inherent and the interdependent threat sources. The methodology is as follows:

- **Establish Investigation Scope:** The investigation scope refers to the systems and the interdependencies that fall under the inspection of the risk analysis exercise.

- **Discover Environmental Dependencies:** The overall consolidation of IT infrastructure has been accompanied by increasing technical linkages and interdependence within and across business. This step is intended to identify all possible interdependent threat sources, through clear examination of environmental dependencies of the system under scope [3]. Environmental dependencies refer to the handshake or communication points of system under scope with the business, technology and operational environments (i.e. development, test, production).

- **Identify Threats and Vulnerabilities:** Based on the inferences derived from the environmental dependencies, this step analyses all potential inherent and interdependent threats and vulnerabilities within investigation scope, by adopting techniques such as manual interpretation, vulnerability scanning and attack simulation.

2.2 Evaluate Risk Probability

The evaluation of risk probability involves estimating through expert judgments, historical event analysis, and by drawing inference from the threat and vulnerability identification step. In [4], the probability of the threat source attacking the system within the investigation scope was analyzed. During early stages of the project, the threat and vulnerability identification exercise reveals significant numbers of newly explored threats, and insufficient historical data are available to enable a complete quantitative analysis. In this situation, one may have to strike a balance between qualitative and quantitative analysis, through expert judgments. Risk probability evaluation methodology includes the followings:

- **Classify and Categorize Risks:** Risk classification is the process of analyzing the threats, discovering related patterns and matches among the threats identified, and classifying the associated patterns into distinct subsets, which are further tagged to a threat clause. Based on the aforementioned classification, one may ascertain that

controlling an independent threat clause would pass along the mitigation to all its interrelated subsets. The threat subsets are further reviewed and categorized against two discrete parameters. These are threats associated with historical events and newly explored threats, for there are unique approaches to calculating the risk probability and cost at risk, which are described in the subsequent risk analysis stages [5].

- **Calculate Risk Probability**: Risk probability involves calculating the probability that the threat source will attack the system under scope, based on the historical events reported over a sampled time period. Risk probability is calculated as an annual estimate and is expressed in percentage scale. The selection of a sample period requires expert Judgement, where reliance has to be placed on factors such as:

  i. The sample time frame reporting of a considerable number of risk events required to perform meaningful analysis.

  ii. The sample time frame's lack of witness to a substantial change to the system under study.

In the event of newly explored threats, one may have to incorporate logical judgements toward calculation of risk probability, as historical analysis could not be performed. The threat classification and the threat type could provide valuable inputs for making judgements. For category of threats associated with historical events, the risk probability is computed as follows; let *RP* denote risk probability, *TRV* total number of risk events reported over a sample period, and *SR* sampled number of years. Then, *RP* is computed as;

$$RP = \frac{TRV}{SR} \times 100 \qquad (1)$$

2.3 Estimation of Cost at Risk

The cost at risk involves estimating the value of damage that the risk event can impose to the system under scope. A tangible estimation technique, with due consideration of direct, indirect and overhead costs, has to be arrived at by an entity by calculating the cost of the risk event. In the case of newly explored threats, the calculation of the cost at risk requires expert judgment, in close liaison with other key elements such as the service impacted and

service commitments. For threats associated with historical events, the cost at risk is computed using the following techniques:

- **Average Restoration Cost**: The average restoration cost is calculated as the average clean-up costs of all threat subsets associated with the threat clause for the sampled time period. By letting *ARC* denote average restoration cost and *SCC*, the sum of clean-up cost; then *ARC* is computed as,

$$ARC = \frac{SCC}{TRV} \qquad (2)$$

- **Cost at Risk**: The cost at risk is the restoration cost computed for the probable number of risk events identified on the system under study. The calculation should follow a bottom-up approach, whereby the cost at risk, pertaining to the threat subsets, is calculated first, followed by the threat clause. The association of the threat clauses with the systems under study can unveil the cost at risk tagged to the overall system [6]. The cost at risk without control, *CRw* is computed as:

$$CR_w = RP \; x \; ARC \qquad (3)$$

2.4 Risk Scoring and Prioritization Tables

Risk prioritization provides a systematic means of prioritizing risks based on the risk exposure rating, which is computed from the inputs received from the risk probability and the cost at risk. The methodology is as follows:

- **Risk Probability Score Table:** The risk probability score table integrates a scoring system to the earlier calculated risk probability values as critical, medium and low, with rankings assigned at each level [7]. Table 1 illustrates a simple risk probability scoring system.

Table 1. Risk Probability Scoring System

Risk probability range	Levels	Numeric score
10% to 25%	Low	1
26% to 60%	Medium	2
> 60%	Critical	3

- **Prepare Cost at Risk Score Table*:*** Similar to the risk probability score table, the cost at risk score table utilizes a scoring system to define high, medium and low cost at risk levels for the earlier computed cost at risk values. Table 2 illustrates a sample cost at risk scoring system.

Table 2. Cost at Risk Scoring System

Cost at risk range	Levels	Numeric score
10% to 25%	Low	1
26% to 60%	Medium	2
> 60%	Critical	3

- **Prepare Risk Exposure Score Table*:*** The risk exposure score is the product of the risk probability score and the cost at risk score.

This is illustrated in Table 3, and it is computed as follows.

$$RE = RP \times CR_w \qquad (4)$$

Table 3. Risk Exposure Scoring System

Risk Exposure	Low cost at risk (1)	Medium Cost at risk (2)	High cost at risk (3)
Low probability (1)	(1,1)		
Medium probability (2)		(2,2)	
Critical probability (3)			(3,3)

- **Risk Prioritization Table**: This involves integrating a scoring system to the risk exposure ratings, where the outcome represents the risk prioritization scores and their corresponding priority levels. Table 4 shows the risk prioritization scoring system.

Table 4. Risk Prioritization Scoring System.

1(LL)	Acceptable	0
2(LM,ML)	Low	1
3(CL,LH)	Medium	2
4(MM)	High	3
6(CM,MH)	Too High	4
9(CH)	Critical	5

2.5 Control Selection

The control selection stage involves the process of determining the appropriate controls and their costs to mitigate the identified risks. The following steps are adopted:

Short List Controls: The short-listing of controls involves planning risk treatment methodologies in controlling the consequences of risk, by mitigating the risk probability. The Methodology is as follows:

- Identify Risk Treatment Plan: The risk prioritization process aids the business in controlling the analyzed risks through risk treatment plans. The risk prioritization table provides the business with an understanding of its current risk exposures and its priorities, which subsequently would help in controlling risks on an organized manner. Some risks are considered potentially destructive, in which case an organization may choose to avoid them completely or it may seek to transfer them. Other risks may be accepted with no further actions, depending on the organization's risk acceptance level [8].

- Short List Suitable Solutions (Controls): The proposed solution might be a single control or a combination of controls, based on the criticality of the risk, where a combination control could be partly preventive and partly detective in nature. In the event that multiple proposed solutions subsist for a particular risk item, the most appropriate ones should be short listed based on cost, adoptability, maintainability and scalability factors.

2.6 Evaluate Residual Risk for the Proposed Control

The computation of residual risk for the proposed control would allow an organization to estimate the overall risk factor that will be mitigated on implementing the said control or solution. If the estimated residual risk level breaches the organization's risk acceptance threshold, the business could

analyze opportunities toward further strengthening the control [1]. The methodology is as follows:

- Identify Control Achieved: Control achieved is calculated through solution analysis of the shortlisted controls. The solution analysis exercise is conducted through an assessment comprised of weighted questionnaire, referencing three key elements such as robustness factor, operational effectiveness factor and resilience factor. The score is further translated to a percentage scale, which characterizes the control achieved.

- Calculate Residual Risk: Controls do not always completely eliminate risk [6]. Any risk remaining after implementing a control is referred to as "residual risk". Though it seems premature to calculate the residual risk before implementing a control, one could estimate the effectiveness of the proposed control by calculating the residual risk based on the previously calculated control achieved value. The logic behind the calculation of the residual risk for the proposed control is to identify the amount of control lost on the probable risk element. The residual risk is calculated thus: let *RR* be residual risk and *C* is control. Then *RR* is computed as;

$$RR = C \times RP \qquad (5)$$

  where Control lost (C) = (1 - % of control achieved)

2.7 Analysis of Cost-Value Proposition

The calculation of cost-value proposition involves evaluation of the cost-benefit of implementing the proposed solution (control). The value derived out of the calculation provides a data-driven decision system for management to realize the cost-benefit of implementing the proposed control [10]. The methodology is as follows:

- **Cost at Risk (with control):** The cost at risk calculated with control provides, as an estimated value of damage, what the risk event can impose to the system under scope after the implementation of the proposed control. The estimation utilizes the input derived from the residual risk toward calculation of the cost at risk with control. Cost at risk with control is calculated thus: Let *CRc* be cost at risk with control and *AVc*, average restoration cost. Then *CRc* is computed as;

Cost at Risk with Control (CR_C) = Residual Risk (RR) x Average Restoration Cost (ARC)

$$CR_c = RR \times ARC \qquad (6)$$

- **Cost of Control:** The cost of control is defined as the sum of the solution cost and the cost at risk with control. The rationale behind this logic is, on selecting the required control, the business has to accommodate the solution cost and the cost at risk with control, since, in most cases, the solution may not control the risk completely and may leave behind some residual risk when, in turn, associates a cost factor to it. If the required solution completely controls the risk without any residual cost, then the cost at risk with control will be zero and the cost of control is equal to solution cost. The solution cost must be expressed as an annual spent value. Any solution has a desired lifetime as any major change or upgrade to business might demand a change or upgrade to the solution, too. The solution lifetime value is a judgmental value specific to a business unit, which, in turn, is driven by the corporation strategy, core functional domain, etc. If the solution lifetime value is ***n*** years, then the overall solution cost has to be approximated to an annual value for calculating the cost of control [10]. Hence, cost of control is calculated thus: let *CC* be cost of control and *SV*, solution cost expressed as annual spent value. Then, *CC* is computed as;

$$CC = CR_c + SV \qquad (7)$$

- **Cost-Value Proposition:** The cost-value proposition is calculated as the difference between the cost at risk without control (calculated during the risk analysis stage) and the cost of control. The logic is a straight forward one. If the outcome of the calculation reveals a positive value, then it is certainly considered cost-effective but if the value is negative, it is not cost-effective, though it needs an expert's decision to analyze the benefit derived from the investment [9]. The cost-value proposition is calculated thus: let *CP* be cost proposition, then *CP* is computed as;

$$CP = CR_c - CC \qquad (8)$$

The outcome of the cost-value proposition provides an effective decision mechanism for the business to focus on, beyond just controlling IT risks, by counterbalancing the value toward controlling the risk [12].

3. DATA COLLECTION

The work explores secondary data collection method; the data were extracted from the risk control documents of HBOS Trading and Investment Company Ltd after a careful and thorough examination. We ensure that data collected were up-to-date and met the standard specification set out in the research work. The risk control documents investigated contained data collected over a period of four years. The data were further categorized, classified and used in our modes; and the results and findings are presented in the section below.

4. FINDINGS AND DISCUSSION

HBOS Trading and Investment Company is a financial going concern. Over the last few years, multiple events were reported on the real-time settlement systems of this financial institution. As a precursor to controlling the risk events, the entity sought assistance from external service providers to review its real-time settlement system and its interface components. A comprehensive threat and vulnerability analysis were performed on the systems under review and their environmental dependencies. The review system within the real-time settlement system scope of investigation had reported three potential risk events over a sample period of four years. The risk events are:

- Frequent real-time settlement software system failure
- Reduction in income generation which may be attributed to risk event 1
- Delayed in authorisation of business processes due to some level manual procedures.

HBOS Trading and Investment Company had already performed the cost estimation of fixing the risk events based on the capital, operational, and resource expenditures. The cost accrued to fixing event 1, event 2, and event 3 was found to be ₦6,300,000.00, ₦546,000.00 and ₦6,020,000.00 respectively. The risk probability of the system under review from our definition in (1) is given as:

$$RP = \frac{TRV}{SR} \times 100$$

Where;

$TRV = 3$

$SR = 4$

$$RP = \frac{3}{4} \times 100 = 0.75 \text{ or } 75\% \qquad (1)$$

The average restoration cost, *ARC* for the system is given as

$$ARC = \frac{SCC}{TRV}$$

Where;

SCC = ₦6,300,000.00 + ₦ 546,000.00 + ₦ 6,020,000.00

= ₦12,586,000.00

$TNR = 3$

$$ARC = \frac{12{,}586{,}000.00}{3} \qquad (2)$$

= ₦4,195,333.33

The annual cost at risk, CR_w is computed as;

$$CR = RP \times ARC \qquad (3)$$

$= 0.75 \times 4195333.33$

= ₦3,146,499.99

The risk exposure score (in monetary term) is therefore computed as:

$$RE = RP \times CR_w \text{ (Without control)} \qquad (4)$$

$= 0.75 \times 3146499.99$

= ₦2,359,874.99

In analyzing the risk probability and the cost at risk elements, one could infer that a risk probability level of 0.75 is positioned at critical level in the risk probability scoring table (system) and a cost at risk value of ₦3,146,499.99 is rated at a high-impact level in cost at risk scoring table (system). The risk exposure score is calculated as critical based on the risk probability and the cost at risk scores.

In continuance to the risk analysis stage, multiple solutions (controls) are proposed towards mitigation of the identified risks for the review system. Based on high-level analysis and judgments, the entity in collaboration with the service providers short-listed a solution (control). This solution (control) is a thorough and complete enhancement of the application software system of HBOS Trading and Investment Company with two alternatives namely: solution 1 (control 1) and solution 2 (control 2) in term of the monetary value needed to build or institute the control. The cost of implementing solution 1 (control 1) for HBOS Trading and Investment Company is ₦21,000,000.00 and solution 2 (control2) is ₦14,000,000.00 based on the control analysis assessment, the percentage control achieved is computed as 82 percent for solution 1 (control 1) and 90 percent for solution 2 (control 2). The residual risk is computed as:

$$RR = C \times RP$$

Where,

Control Lost = 1 - % of control achieved

= (1 – 0.82) for solution 1 (control 1) and

= (1 – 0.90) for solution 2 (control 2)

Therefore,

$$RR = (1 - 0.82) \times 0.75$$

$$= 0.135$$

That is, 13.5% for solution 1 (control 1). For solution 2 (control 2), we have,

$$RR = (1 - 0.90) \times 0.75 \qquad (5)$$

$$= 0.075$$

That is, 7.5% for solution 2 (control 2).

The cost at risk (with control) is computed as follows:

For solution 1 (control 1), cost at risk with (control) is computed as

$$CR_c = RR \times AVC \quad (6)$$

$$CR_c = 0.135 \times 4195333.33$$

$$= ₦566369.99$$

Based on judgments, the service providers found the solution life for HBOS Trading and Investment Company's business environment to be at least four years. Hence, the solution (control) cost corrected to annual scale for solution 1 (control 1) is equal ₦21000000.00/4 = ₦5250000.00.

For solution 2 (control 2) is ₦ 1400000.00/4 = ₦350000.00. Then, the cost of control for the two solutions (controls) is computed as follows:
For solution 1 (control *1*);

$$CC = CR_c + SV$$

$$= ₦566369.99 + ₦5250000.00$$

$$= ₦5816369.99$$

For solution 2 (control 2);

$$CC = CR_c + SV \quad (7)$$

$$= ₦566369.99 + ₦350000.00$$

$$= ₦916369.99$$

Hence, the cost value proposition for the two solutions (*controls*) is calculated as follows: For solution 1 (control 1);

$$CP = CR_c - CC \quad (8)$$

$$= ₦3146499.99 - ₦5816369.99$$

$$= ₦ -2,669,870.00$$

For solution 2 (control 2);

$$CP = CR_c - CC$$

$$= ₦3146499.99 - ₦916369.99$$

= ₦2,230,130.00

As per the values derived out of the cost-value proposition step, solution 2 (control 2) reveals a positive cost-value and solution 1 (control 1) reveals a negative cost-value. A positive cost-value outcome provides an encouraging rationale toward selection of the solution (control).

5. CONCLUSION

The current business environment demands that business services delivered by businesses must be information technology (IT) based. For businesses to remain active in the competitive environment, they need to stay abreast of managing their information technology (IT) risks effectively, and this can be done by adopting the data-driven technique.

REFERENCES

[1] Rameshkumar, A. V. Looking IT Risk Differently. *ISACA Journal*, *1* (2010), 10 -12.

[2] Bowman, B., Debray, S. K., and Peterson, L. L. Reasoning about naming systems. *ACM Trans. Program. Lang. Syst., 15*, 5 (Nov. 1993), 795-825.

[3] Harold, T. and M. Krouse, M. *Information Security Management Handbook*, 6th Edition, Auerback Publications, 2007.

[4] G. Singleton, G. and Tommie, W. What Every IT Auditor should know About Auditing Information Security. *Information Systems Control Journal*, *2* (2007), 6 – 9.

[5] Jackub, M. A Service-Oriented Approach to Identification of IT Risk. *Proceedings of the TEHOSS' 2005 first IEEE International Conference on Technologies for Homeland Security and Safety*, 2005, 10 – 11.

[6] Champlain, J. *Auditing Information Systems, John Wiley & Sons Inc., 2003.*

[7] Sathiyamurthy, S. Is the IT Risk Worth a Control? Defining a Cost-Value Proposition paradigm for Managing IT Risks. *Information Systems Control Journal, 6* (2006), 14 -16.

[8] Srinivas, S. Continuous Auditing through leveraging Technology. *Information Systems Control Journal, 2,* (2006), 3 – 6.

[9] Urs, F. Risk IT: Based on COBIT objectives and principles. *ISACA, 4*, (2009), 21 -23.

[10] Westerman, G. and Hunter, R. IT Risk: Turning Business Threats into Competitive Advantage. *ISACA and IT Governance Institute, Illinois*, (August 2007), 54 – 66.

[11] Vona, L. W. Fruad Risk Assessment: Building a Fraud Audit Program *ISACA and IT Governance Institute., Illinois*, (August 2008), 16 – 26.

[12] F. K. Reilly, F. K. and Brown, K. *Investment Analysis and Portfolio Management*, 12-18, Harcourt College Publisher, Illinois, (July 2002),

[13] D. L. Canon, D. L. *Certified Information Systems Auditor (CISA) study guide*, 3rd Edition, March 2011.