International Journal of Accounting Information Systems, Volume 10, Number 2, pp. 65-78.

An Evidential Reasoning Approach to Sarbanes-Oxley Mandated Internal Control Risk Assessment

Theodore J. Mock[1], Lili Sun[2], Rajendra P. Srivastava[3], and Miklos Vasarhelyi[2]

[1]Anderson Graduate School of Management, University of California, Riverside, CA, 92521, USA
[2]Department of Accounting and Information Systems, Rutgers University-Newark, NJ, 07102, USA
[3]School of Business, The University of Kansas, Lawrence, KS, 66045, USA

[1]tmock@marshall.usc.edu, [2]sunlili@rbsmail.rutgers.edu, [3]rsrivastava@ku.edu,
[4]miklosv@andromeda.rutgers.edu

Abstract

In response to the enactment of the Sarbanes-Oxley Act 2002 and of the release of the Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 5, this study develops a risk-based evidential reasoning approach for assessing the effectiveness of internal controls over financial reporting (ICoFR). This approach provides a structured methodology for assessing the effectiveness of ICoFR by considering relevant factors and their interrelationships. The Dempster-Shafer theory of belief functions is utilized for representing risk.

First, we develop a generic ICoFR assessment model based upon a Big 4 audit firm's approach and apply it to a real-world example. Then, based on this model, we develop a quantitative representation of various levels of ICoFR effectiveness and related risk-assessment as defined by the PCAOB and contrast these representations with levels implied by Auditing Standard No. 5. In doing so, we demonstrate the potential value of formal risk assessment models in both facilitating the assessment of risks in an individual engagement and in assessing the effects of different regulations.

Keywords: Sarbanes-Oxley (SOX), PCAOB Audit Standard No. 5, Internal Control over Financial Reporting, Evidential Reasoning, Risk-Assessment, Theory of Belief Functions.

1. Introduction

Internal control evaluation is a risk-assessment process (PCAOB Audit Standard No. 5) utilized by both a firm and its auditor to assess various aspects of the firm's accounting information system. Accounting internal control systems which are affected by an entity's board of directors, management, and other personnel are designed to provide reasonable assurance regarding the effectiveness and efficiency of operations, the reliability of financial reporting, and compliance of the organization with laws and regulations (COSO, 1992). The importance of effective internal controls has long been recognized in the auditing literature (Mautz and Sharaf 1961). Effective internal control

can help companies achieve established financial goals, prevent loss of resources, keep accurate recording of transactions, and prepare reliable financial statements (Ernst & Young 2002).

The Sarbanes-Oxley Act of 2002 (the Act) has resulted in renewed attention to internal controls over financial reporting (ICoFR). The act makes reporting on internal controls mandatory for SEC registrants and their independent auditors. Section 404 of the Act directs the SEC to adopt rules requiring annual reports of public companies to include an assessment, as of the end of the fiscal year, of the effectiveness of internal controls and procedures for financial reporting. Section 404 also requires the issuer's independent auditors to attest to and report on management's assessment. Section 302(a) of the act requires that the CEO and CFO must assess the effectiveness of the issuer's disclosure controls and procedures, of which ICoFR are a part. In May, 2007 the PCAOB released Audit Standard No. 5 which encourages a 'risk-based' implementation of Sections 404 and 302(a). This paper develops and illustrates a framework that may be used in such an implementation.

Throughout the post-SOX era, both auditors and their clients have been concerned with the provision of an effective and efficient evaluation of ICoFR. However, in the period following the enactment of SOX up to the present, the fulfillment of Section 404 ICoFR assessment has imposed heavy burdens on external auditors and management. For example, both the business press and academic research (e.g., Ettredge et al. 2006) suggest that companies have experienced significantly longer audit delay due to SOX 404-compliance, which has made it more challenging to implement the Security Exchange Commission's (SEC) 60-day filing deadline. Research also has shown that investors tend to react negatively to longer audit delays (e.g., Chambers and Penman 1984). Further, the announcement of a material weakness in internal control systems has been associated with drops in stock price, increased share volume, and even some CFOs losing their jobs (Durfee 2005).

All of these possible effects of providing assurance under SOX 404 indicate that being able to effectively and efficiently evaluate ICoFR, to quickly identify the major weaknesses in control systems, and to quickly take remedial actions to fix these weaknesses is critical. A structured and systematic approach to SOX 404 mandated internal control assessment could help in achieving such a goal. This paper, by proposing such a methodology and demonstrating its application, presents an approach that should be helpful to the assurance provider, to management and to regulators.

Both qualitative and quantitative methods exist for the evaluation of internal controls (IC). Conventionally, auditors have adopted qualitative methods, such as questionnaires, checklists, flow charts, and test of transactions for evaluation purposes. Previous research (*e.g.* Yu & Neter 1973; Cushing 1974, 1975; Mock & Turner, 1981) point out that such methods are ineffective and the assessments generated by qualitative methods are of dubious values for developing comprehensive internal control evaluation models. Alternatively, a number of quantitative methods, including both a stochastic model (Yu & Neter 1973), and a reliability model (Cushing 1974) were developed and improved upon by several researchers (e.g., Grimlund 1982; Srivastava

and Ward 1983; Srivastava 1986). Unfortunately, research on IC assessment methods has been somewhat scarce in the past decade. And, none of the cited approaches provide an appropriate basis for SOX 404 assessment.

The methodology proposed by this study is an evidential reasoning approach which is based upon the Dempster-Shafer theory of Belief Functions. This approach provides a systematic way to represent the interrelationships among key accounting system components for the evaluation of ICoFR, including significant accounts being evaluated, business processes impacting these accounts, risks to which business processes are exposed, control procedures implemented to counter the risks, and evidence gathered to evaluate the effectiveness of control procedures.

Given judgments on strength of the audit evidence gathered as input, the proposed method provides a rigorous algorithm to aggregate these judgments, propagate and aggregate the results, and output quantitative risk assessments on various levels within the accounting information system. Included are assessments related to the overall ICoFR, significant accounts level, business process level, individual risk level, and individual control procedure level. These detailed quantitative representations provide important information upon which both management and auditors can make inferences on the effectiveness of ICoFR at both the overall financial statement level and various more detailed levels. Such information is also valuable in facilitating the process of identifying any major weaknesses existing in the IC system, and for optimizing the value of IC investment.

As noted, the main objective of this study is to propose and demonstrate the implementation of an evidential reasoning approach for an efficient and effective risk assessment of ICoFR. We attempt to achieve this objective through addressing the following important research questions:

1. What is an appropriate definition of internal control risk?

2. What is the generic structure of an ICoFR risk assessment model?

3. What is an appropriate mapping rule between the model's quantitative representations and alternative assessment opinions (e.g., effective, ineffective, significant deficiency, material weakness)?

4. What are appropriate representations of an accounting information system and the relationships among financial statement assertions?

5. What is an appropriate way of assessing the expected value of the addition of various controls and safeguards on risks?

6. How has the release of PCAOB Auditing Standard No.5 altered the requisite risk assessments?

To address these research questions, the remainder of the paper is divided into the following sections. Section 2 introduces the theoretical foundation of the evidential

reasoning approach. Section 3 defines internal control risk, and develops a generic evidential reasoning model for IC assessment. Section 4 illustrates the use of the generic model based on a real SOX 404 case, and discusses how to quantitatively represent varying levels of ICoFR effectiveness. This section also attempts to assess the impact of several features of PCAOB Auditing Standard No.5 on the assessments. The last section concludes the paper.

2. Evidential Reasoning Approach under Dempster-Shafer (DS) Theory of Belief Functions

The evidential reasoning approach under the Dempster-Shafer (DS) theory of belief functions has been widely used in a broad range of disciplines (e.g., see, Srivastava and Mock 2002),. Examples directly related to accounting information systems and auditing include applications in audit and assurance services (e.g., Srivastava and Shafer 1992; Shafer and Srivastava 1990; Srivastava and Mock 2000), artificial intelligence and expert systems (e.g., Gordon and Shortliffe 1984; Xu, Hsia and Smets 1993), data mining and information systems security evaluation (e.g., Wilkins and Lavington 2002; Sun, Srivastava, and Mock 2006), and financial portfolio management (Shenoy and Shenoy 2002).

Basically, this evidential reasoning approach is a process of risk assessment where several variables (assertions) when combined together inform us about a variable of interest such as the effectiveness of internal control. It allows the decision maker to develop a framework that aggregates all the evidence available in the situation pertaining to various intermediate variables and then infer about the variable of interest. Such a feature makes the approach appealing to the evaluation of the effectiveness of the ICoFR system because the ultimate effectiveness relies upon multiple factors such as the effectiveness of multiple control procedures, the control environment, and evidence gathered from various sources.

Rather than using probabilities to represent uncertainties, we use belief functions to represent uncertainty in the evidential reasoning approach. Belief functions theory was made popular by Shafer (1976). It is a generalization of Bayesian theory and unlike probability theory it represents ignorance as a separate explicit component of the evaluation. There are three basic functions that are important to understand the use of belief functions in a decision-making process: *m-values*, *belief functions*, and *plausibility functions*. Dempster's rule is the fundamental rule similar to Bayes' rule in probability theory for combining items of evidence. Appendix A elaborates on the basic concepts[1].

3. A Generic Evidential Reasoning Model for Sarbanes-Oxley Mandated Internal Control Assessment

3.1 Definition of Internal Control Risk

[1] Readers are suggested to refer to Srivastava and Mock (2002) and Yager et. al (1994) for more elaboration and applications of Belief Function theory.

The proposed approach defines ICoFR risk as the plausibility that deficiencies in ICoFR systems result in more than a remote likelihood that a material misstatement within the annual or interim financial statements will not be prevented or detected. According to the PCAOB, there is a hierarchy of possible deficiencies: control deficiency; significant deficiency, and material weakness. How do we tie our ICOFR risk definition to this hierarchy? In the present paper, we define two possible states of a control system; either the control system is effective (e) or ineffective (~e) in controlling the possible errors in accounting for financial transactions. In addition, we consider that if the control system is ineffective then there are three possible conditions of ineffectiveness: deficiency, significant deficiency, and material weakness. These conditions depend on how sever the deficiency is. We elaborate this approach below.

As mentioned earlier, we use the plausibility that the control system is ineffective as the definition of control risk. Srivastava and Shafer (1992) have used a similar definition in defining audit risk as the plausibility of material error in the financial statements. Sun et al (2006) have used it to define information security risk as the plausibility that the information system is not secure. We use the following set of m-values and the corresponding plausibilities, to define four levels of effectiveness and ineffectiveness (deficiency, significant deficiency, and material weakness) of a control system.

***Effective Control System*:**

$m(e) \geq 0.90$, $m(\sim e) \leq 0.1$, i.e., $Pl(\sim e) \leq 0.1$, and $Bel(\sim e) \leq 0.1$.

***Deficient Control System*:**

$0.9 \geq m(e) \geq 0.70$, $m(\sim e) \leq 0.30$, i.e., $0.1 \leq Pl(\sim e) \leq 0.30$, and $Bel(\sim e) \leq 0.30$.

***Significantly Deficient Control System*:**

$0.70 \geq m(e) \geq 0.50$, $m(\sim e) \leq 0.5$, i.e., $0.30 \leq Pl(\sim e) \leq 0.5$ and $Bel(\sim e) \leq 0.50$.

***Materially Weak Control System*:**

$0.5 \geq m(e)$, $m(\sim e) \geq 0.5$, i.e., $Pl(\sim e) \geq 0.5$, and $Bel(\sim e) \geq 0.50$.

Note that there is obvious flexibility in these definitions and the stated ranges and thresholds can be altered to suit the particular audit firm risk preferences and client situation. However, the following arguments provide support for using the above definitions as a starting point. First, a system of ICoFR is *effective* if the belief mass, i.e., m-value, that it is effective exceeds a threshold level, say 0.9. This means that if the evidence related to a control effectiveness suggests that $m(e) \geq 0.90$, we define that system to be effective. The corresponding belief mass that the control system is ineffective may be equal to or less than 0.1, i.e., $m(\sim e) \leq 0.1$. These values yield the plausibility that the control system is ineffective to be less than 0.1, i.e., $Pl(\sim e) \leq 0.1$.

A system of ICoFR is defined as *deficient* when the evidence suggests that the belief mass that it is effective is not as high as the threshold of effective control, but at the same time there is substantial evidence that it is effective. This is the reason we assume the belief mass in support of its effectiveness to be between 0.9 and 0.70, i.e., $0.9 \geq m(e) \geq 0.70$. In this case, the assessed belief related to possible ineffectiveness of the control system may be less than 0.30, i.e., $m(\sim e) \leq 0.30$. The above definition of an effective system of ICoFR and these m-values yield a value for the plausibility that the control is not effective to be between 0.1 and 0.30, i.e., $0.1 \leq Pl(\sim e) \leq 0.30$. In other words, the control system is assessed to be *deficient* if the control risk is between 0.1 and 0.30, and the belief that the control system is ineffective is less than 0.30, i.e., $Bel(\sim e) \leq 0.30$.

A system of ICoFR is *significantly deficient* if the evidence suggests that the belief associated with the control system being effective is at a medium level between 0.70 and 0.5, i.e., $0.70 \geq m(e) \geq 0.50$, and the belief mass that the control system is not effective is below 0.5, i.e., $m(\sim e) \leq 0.5$. These m-values yield a values of the plausibility that the control system is not effective between 0.3 and 0.5, i.e., $0.3 \leq Pl(\sim e) \leq 0.5$. This suggests that a control system is *significantly deficient* if the control risk is between 0.3 and 0.5 and the belief that the control is not effective is less than 0.50, i.e., $Bel(\sim e) \leq 0.50$.

Lastly, a system of ICoFR is *materially weak* when the evidence suggests that the belief associated with the control system being effective is low, say below 0.5, i.e., $m(e) \leq 0.5$ and the belief related to the ineffectiveness of the control system is greater than or equal 0.5, i.e., $m(\sim e) \geq 0.5$. These m-values yield a value for the plausibility that the control system is ineffective that is greater than 0.5, i.e., $Pl(\sim e) \geq 0.5$. This definition implies that the control system should be classified as *materially weak* when the control risk is greater than 0.5 and the belief that the control is ineffective is greater than 0.5, i.e., $Bel(\sim e) \geq 0.50$. Again, we note that these ranges and thresholds may be altered depending on the client situation and the risk profile that assurance provider is willing to accept.

3.2 Structure of the Generic Model

The generic evidential reasoning model developed here is based upon a Big 4 firm's model of risk assessment as implemented under Auditing Standard No. 2 (PCAOB 2004). Potential modifications based on Auditing Standard No. 5 (PCAOB 2007) are then considered to illustrate some of the useful features of the model.

The generic risk assessment model sketched in Figure 1 consists of a financial reporting part and a business process part. The financial reporting part depicts the hierarchy of the following main components from the left to the right: parent company, subsidiary company, and the significant accounts on financial statements. The 'hierarchy' relates to the aggregation of control risk assessments from the significant accounts to the overall consolidated entity. The business process part consists of the management assertions concerning the ICoFR system pertinent to the significant

accounts, risks associated with these assertions, and the control procedures implemented to mitigate these risks. Thus, internal controls are designed to control risks specific to management's assertions concerning the accounting information system effectiveness.

As depicted in Figure 1, the structure of the generic, evidential reasoning model proposed here corresponds to the risk assessment model of a Big 4 auditing firm. In the model, the main assertion to be evaluated is "The system of internal control over financial reporting (ICoFR) for the consolidated entity is effective". Since the effectiveness of ICoFR at the consolidated entity level depends upon the effectiveness at each subsidiary, the system of ICoFR for each subsidiary being effective is expressed as a first-level sub-assertion. To examine whether the system of ICoFR for subsidiary *i* is effective, an assessor should examine the effectiveness of the IC related to significant accounts. An account is significant if it could contain material errors. The second level sub-assertion states that "The system of ICoFR for a significant account (e.g., cash) is effective". These are the main components of the financial reporting component of the generic model.

The remaining part of the proposed model is the business processes component that relates to a specific management assertion. Assertions, including the main assertion and sub-assertions, are represented by rounded boxes in the evidential diagrams. In this part of the model, the traditional idea of controls over financial accounts is elaborated by adding several layers of sub-assertions between the financial accounts and the actual controls. The effectiveness of each significant financial account depends on whether each of several multiple assertions is valid or not. Typical assertions to be considered are "Existence", "Completeness", "Valuation" and "Presentation" (see AU Sec. 326, *Evidential Matter*).

Broadly speaking, for each management assertion, we have several potential risks, and for each risk there may be more than one internal control to mitigate the risk. In the model, the third level sub-assertion is expressed as "The system of ICoFR for a management assertion related to a financial account is effective". Each assertion may be threatened by one or more risks. Thus for a system to be effective a number of fourth level sub-assertions expressed in general as "An assertion is protected from an ICoFR risk" must be true. Every risk can be mitigated by one or more controls. The existence and effectiveness of each control is expressed as the fifth level sub-assertion.

The generic model provides the baseline structure for the implementation of the proposed approach. The baseline structure is adaptable to a user's specific situation and interest, since it allows users to add additional assertions, and to modify or delete existing assertions in the generic model.

Relationships among the main assertion and the first level to the fourth level sub-assertions are represented by "and" relationships. An 'and' relationship implies that the higher level assertion or sub-assertion is true if and only if each lower level sub-assertion is true. One or more internal controls can be implemented to protect a process related to a management assertion from a risk. If controls are compensating to each

other, a process is protected from a risk if some controls (but not necessarily all of controls) are effective. Therefore, the relation between compensating controls is represented by the “or” relationship, which implies the higher level sub-assertion is true if any of the lower level sub-assertions is true. If controls are not compensating, the overall assessment of internal control pertaining to the management assertion is not effective unless all controls pertaining to it are functioning effectively. Therefore, non-compensating controls are linked through the “and” relationship. In Figure 1, each fourth level sub-assertion is connected through an “and/or” relationship with the related fifth level sub-assertions. Thus, which relationship is appropriate is dependent upon the nature of controls.

Evidence, represented by a rectangular box, is information obtained to support or negate one or multiple assertions. Evidence nodes are connected to the corresponding assertion(s) (the main assertion or any sub-assertion) that they directly pertain to.

One or multiple evaluation procedures can be performed to evaluate the effectiveness of a control. Evaluation procedures produce items of evidence which support, negate, or support and negate (i.e. mixed evidence) control effectiveness. The degree of support or negation is represented by the strength of evidence, the assessment of which requires expert judgments. Often, one evaluation procedure provides support or negation to more than one control.

Given that evidence should pertain to the assertion(s) it directly supports or negates, evidence can be located at various layers of the model. In Figure 1, evidence that directly pertains to the effectiveness of controls is connected to the various fifth-level sub-assertions which assert the effectiveness of a particular control procedure.

Evidence related to a higher level assertion in the model such as the organizational control environment helps evaluate management’s attitude toward the development of accounting estimates, its financial reporting philosophy, and the context in which the accounting system and internal controls operate. For example, evidence concerning the client’s ‘control policies & procedures’ will have an impact on multiple sub-assertions and therefore is connected to the main assertion. As noted, evidence nodes are represented by rectangular boxes in the evidential diagrams.

3.3 Algorithm for evidence aggregation

In this study, the Dempster-Shafer theory of belief functions is employed to assess, aggregate and propagate the evidence within the model. As Shenoy and Shafer (1990) have discussed, the aggregation process becomes quite complicated as the model grows. However, there are several software packages available (see, e.g., Shafer et al. 1988, Zarley, et al. 1988, and Saffiotti and Umkehrer 1991) that facilitate the aggregation and propagation process. Recently, Srivastava (2005) has developed an alternative form of Dempster’s Rule of combination which allows one to easily program the logic in MicroSoft Excel spreadsheets to compute the combined m-values for a large number of independent items of evidence. Also, Srivastava et al (1995) have developed analytical formula for combining items of evidence in an “and” tree which is a typical

evidential diagram for assessing internal controls. These two developments greatly enhance the proposed approach's practicability and simplicity of use. In the paper, the computation is conducted in Excel using the formula developed by Srivastava (2005) and Srivastava et al (1995).

4. Extending the Generic Evidential Reasoning Model for Sarbanes-Oxley Mandated Internal Control Assessment Based on Auditing Standard No. 5 Assumptions

In this section, we demonstrate the approach by applying it to a real engagement from one of the Big Four auditing firms. The actual engagement was conducted when Standard No. 2 was in force. Then we consider some differences that would have occurred if the analysis had been conducted under Standard No. 5.

In this engagement, the auditing firm provided advisory services to a client in the financial industry concerning the client's responsibilities under SOX 404 requirements. We obtained the client's financial statements and documentation of all business processes related to management assertions, business risks, control procedures implemented, and the auditing firm's evaluation of the control procedures.

The original documentation provided a large volume of information. To simplify the illustration discussed here, we developed an evidential reasoning model for the ICoFR evaluation related to the most significant account on the company's balance sheet: "Net Loans". The baseline model is depicted in Figure 2 in a form similar to Figure 1. The unaudited value of this account was $28.9 billion, clearly a material amount for this company.

4.1 An Assessment of Beliefs and ICoFR Risks under Auditing Standard No. 2

Auditing Standard (AS) No. 5 demonstrates how to incorporate knowledge accumulated from prior years' audits into the assessment of ICoFR. According to AS No. 5, auditors should consider the significant controls that would prevent and detect material misstatements in the account being considered. In addition, when deciding about the extent, nature, timing and staffing of testing the internal controls, the auditor should consider prior year's assessments of the internal controls and also use the work of the others based on the effectiveness and objectivity of the other sources. For example, the auditor can use both the prior year experience and also the internal auditor's assessment of the internal controls when deciding the extent, nature and timing of controls tests. One way an analytical model such as that presented in this paper can be useful is to help regulators and others analyze the effects of such changes in standards. The Research Question that this leads to is:

RQ1: How does each change in a standard affect the assurance provider's risk assessments and the efficiency and effectiveness of the engagement?

The shaded items of evidence in Figure 2 are the ones that are to be considered under AS No. 5. Since these items of evidence may not have been considered in the actual

engagement which was conducted under AS No. 2, the input values for these items of evidence were zero belief that controls are effective and zero belief that the controls are ineffective in Figure 2. In other words, these items of evidence do not exist under AS No. 2.

Figure 3 represents the situation under AS No. 5. Here we assume the auditors have formally considered the following items of evidence: 1) prior year (PY) experience with the internal controls, 2) use the work of others such as internal auditors (IA), and 3) evidence about controls at the entity level and at the individual account level. These items of evidence are depicted in Figure 3.

There is no well-accepted rule in terms of the quantitative belief representation for various levels of IC effectiveness. In Table 1 we show the assumed m-values as the auditors' evaluation on the effectiveness of individual control procedure using the classification schemes defined in the previous section. As noted, these values can be changed according to the audit firm's preferences. Importantly, one feature of an analytical model such as that illustrated in this paper is that sensitivity analysis can be performed to evaluate the effects on the assessments of ICoFR of different assumptions as to what constitutes effective and ineffective control.

Table 1: Types of Internal Control Effectiveness Defined in Terms of Belief Values.

Internal Control effectiveness	Strength of evidence				
	Belief that the control is effective, m(e)	Belief that the control is ineffective, m(~e)	Uncommitted Belief as to whether control is effective or not, m({e, ~e})	Control Risk, Pl(~e)	Belief that Control is effective and ineffective
Control is Effective	0.98	0.00	0.02	0.02	Bel(e) = 0.98 Bel(~e) = 0
Control is Deficient	0.70	0.10	0.20	0.3	Bel(e) = 0.7 Bel(~e) = 0.10
Control has Material Weakness	0.00	0.90	0.10	1.0	Bel(e) = 0 Bel(~e) = 0.9
Unknown	0.00	0.00	1.00	1.0	Bel(e) = 0 Bel(~e) = 0

Based upon an "and" relationship, after aggregating all items of evidence, the model in Figure 2 (Prior to AS No. 5) suggests that there is zero belief that the IC on the 'Net Loan' account is effective, 91% belief that the IC on the 'Net Loan' account is ineffective, and 9% of ambiguity indicating that it is unknown whether the IC is effective or not. If we use the same mapping rule as suggested above, the overall assessment opinion suggested by the model would be that the overall IC on 'Net Loan' has a material weakness. Although Figure 3 yields a similar conclusion, the assessment process is much more efficient because of the consideration of the other items of

evidence such as the prior year experience, the work of internal auditors, and giving consideration to the entity level controls and the account level controls. As one can see from Figure 3, the level of belief that needs to be obtained from the tests of control is lower than the level desired without these additional items of evidence. This illustrates one use of the model presented in this paper, which is an explicit assessment of the change in the risk assessments that result from collecting additional audit evidence.

If such evidence is already available (for example, based on prior years audits), then the auditor needs to do less work in the current year to obtain the same level of overall confidence whether the controls are effective or not. Thus, it appears that the implementation of AS No. 5 ought to lead to cost savings in providing assessments on internal controls.

4.2 Assessment of Beliefs and ICoFR Risks under Auditing Standard No 5

AS No. 5 focuses on 'risk' rather than 'coverage'. This change may be interpreted as leading to adding some branches of the baseline evidential network sketched in Figure 2 and leads to our second research question:

> RQ2: How does a 'risk-based' approach under AS No. 5 for assessing ICoFR risks affect the assessed beliefs and risks and affect the efficiency and effectiveness of the audit in comparison to a 'coverage-based' approach under AS No. 2?

As mentioned earlier, Figure 3 depicts the evidential diagram for the audit process under AS No. 5 whereas Figure 2 depicts the evidential diagram for the audit process under AS No. 2. The main difference between the two approaches is that under AS No. 2, the auditor was supposed to evaluate each pertinent internal control through performing control tests and not consider the evidence from the prior year (PY) or not use the work of others such as internal auditors (IA). Although these procedures are depicted as items of evidence in Figure 2 as rectangular boxes, they are not performed as shown by shaded boxes (the input values are zero for and against the IC being effective). In Figure 3, these procedures are performed (not shaded any more), i.e., the auditor considers these additional items of evidence. The assessed input beliefs by the auditor based on PY knowledge about the internal controls and based on IA are input in the evidential diagram. As seen from the input values in Figure 3, these values are relatively small in favor of IC being effective (from 0.1 to 0.3) except in one case it is small, 0.1, but against the IC being effective. The evidence at the higher level assertions coming from assessing the control environments is assumed to be 0.2 and 0.5, respectively, in support of the corresponding internal control assertion. The effect of these additional procedures is that the level of belief desired from control tests for each specific internal control is at a lower level than what was desired to obtain the same level of overall confidence as in the evidential diagram based on AS No. 2.

The above findings suggest that not only the assessed risk and beliefs based on the prior year knowledge of the internal controls and the knowledge about the control environment reduce the desired level of beliefs from the control tests and hence make

the process more efficient, but also, in effect, reduce the cost of performing these tests of controls as a result of reduced desired level of beliefs and thus making the process more cost effective.

5. Conclusions

The fulfillment of SOX Section 404 requirement of ICoFR imposes heavy burdens on auditors and management. In the period when AS # 2 was in effect, many companies had difficulties meeting the SEC deadlines and in providing appropriate control documentation. We argue that an appropriate methodology for ICoFR evaluation such as that suggested and illustrated here, may help facilitate Section 404 compliance.

This paper has developed an evidential reasoning approach under Dempster-Shafer (DS) Theory of Belief Functions for the assessment of ICoFR. We discuss the theoretical ground of the approach, develop a generic evidential reasoning model, and further demonstrate the model using a real example. The approach provides a structured manner to incorporate key assessment factors and their interrelationships when estimating ICoFR risk. It provides a rigorous algorithm to aggregate an assessor's beliefs. The approach helps discipline the assessor's thought process in estimating IC risk and may serve as a useful decision aid for auditors and management to conduct an effective and efficient evaluation on ICoFR.

In addition, an analysis of the proposed model for two scenarios, prior to AS No 5 and post-AS No 5, suggests that the implementation of AS No 5 should lead to more efficient evaluation of internal controls' effectiveness and thus would lead to a significant cost saving.

REFERENCES

Chambers, A. E., and Penman S. H. (1984), Timeliness of Reporting and the Stock Price Reaction to Earnings Announcements. *Journal of Accounting Research* Vol. 22, No. 1, pp. 21–47.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO). (1992), *Internal Control-Integrated Framework*.

Cushing B. E. (1974), "A Mathematical Approach to the Analysis and Design of Internal Control Systems", *The Accounting Review,* Vol. 49, No. 1, pp. 24-41.

Cushing B. E. (1975), "A Further Note on the Mathematical Approach to Internal Control", *The Accounting Review*, Vol. 50, No. 1, pp. 151-154.

Dempster A. P., Yager R. R., and Liu L. (2008), *The Classic Works on the Dempster-Shafer Theory of Belief Functions*, Springer-Verlag.

Durfee D. (2005), "The 411 on 404: Reporting a material weakness in controls can cost shareholders millions and some CFOs their jobs", *CFO Magazine*.

Ettredge M., Li C., and Sun L. (2006), "The Impact of SOX Section 404 Internal Control Quality Assessment on Audit Delay in the SOX Era", *Auditing: A journal of Practice and Theory*, Vol. 25, No. 2, pp. 1-23.

Ernst & Young LLP. (2002), “Preparing for Internal Control Reporting: A Guide for Management’s Assessment Under Section 404 of the Sarbanes-Oxley Act”.

Gordon J., and Shortliffe, E. H. (1984), “The Dempster-Shafer theory of evidence. In, B.G. Buchanan and E.H. Shortliffe, (eds.), *Rule-Based Expert Systems: The MYCIN Experiments of the Stanford Heuristic Programming Project*, Addison-Wesley.

Grimlund R. A. (1982), “An Integration of Internal Control System with Account Balance Evidence”, *Journal of Accounting Research*. Autumn pt. I, pp. 316-342.

Mautz R. K., and Sharaf H. A. (1961), *The Philosophy of Auditing*, American Accounting Association.

Mock T., and Turner J. (1981), Internal accounting control evaluation and auditor judgment, American Institue of Certified Public Accountants, New York, NY, USA.

Public Company Accounting Oversight Board (PCAOB). (2004), An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements. Auditing Standard No. 2.

Public Company Accounting Oversight Board (PCAOB). (2007), An Audit of Internal Control Over Financial Reporting that is Integrated with an Audit of Financial Statements and Related Independence Rule and Conforming Amendments. Auditing Standard No. 5.

Saffiotti A., and Umkehrer E. (1991), “Pulcinella: A General Tool for Propagating Uncertainty in Valuation Networks”*. Proceedings of the Seventh National Conference on Artificial Intelligence,* University of California, Los Angeles, pp. 323-331.

Shafer G. (1976). *A Mathematical Theory of Evidence*, Princeton University Press.

Shafer G., and Srivastava R. P. (1990), The bayesian and belief-function formalisms: a general perspective for auditing. *Auditing: A Journal of Practice and Theory*, (Supplement), pp. 110-148.

Shafer G., Shenoy P. P., and Srivastava R. P. (1988), “AUDITOR'S ASSISTANT: A Knowledge Engineering Tool For Audit Decisions”, *Proceedings of the 1988 Touche Ross/University of Kansas Symposium on Auditing Problems,* May, pp. 61-79.

Shenoy and Shafer (1990), “Axioms for Probability and Belief-Function Propagation”. In R. D. Shachter, T. S. Levitt, L. N. Kanal and J. F. Lemmer (eds.), *Uncertainty in Artificial Intelligence,* Vol. 4, pp. 169—198.

Shenoy C.; and Shenoy, P. P. (2002), “Modeling financial portfolios using belief functions”. In, Srivastava, R. P. and Mock, T., (eds.), *Belief Functions in Business Decisions,* Heidelberg, New York: Physica-Verlag, pp. 316-332.

Srivastava R. P. (1986), “Auditing Functions for Internal Control Systems with Interdependent Documents and Channels”, *Journal of Accounting Research,* Vol. 24, No. 2, pp. 422-426.

Srivastava R. P. (2005), “Alternative Form of Dempster’s Rule for Binary Variables. *International Journal of Intelligent Systems*, Vol. 20, No. 8, pp. 789-797.

Srivastava R. P., and Shafer G. (1992), “Belief-Function Formulas for Audit Risk”. *The Accounting Review*, Vol. 67, No. 2, pp. 249-283.

Srivastava R. P., Shenoy P.P., and Shafer G. (1995), “Propagating Beliefs in an 'AND' Tree”, *International Journal of Intelligent Systems,* Vol. 10, pp. 647-664.

Srivastava R. P., and Mock T. (2000), “Evidential reasoning for WebTrust assurance services”, *Journal of Management Information Systems,* Vol. 16, No. 3, pp. 11-32.

Srivastava R. P., and Mock T. (2002), *Belief Functions in Business Decisions,* Physica-Verlag, Heidelberg, Springer-Verlag Company.

Srivastava R. P., and Shafer G. R. (1992), “Belief-Function Formulas for Audit Risk”, *The Accounting Review*, Vol. 67, No. 2, pp. 249-283.

Srivastava R. P., and Ward B. H. (1983), “Reliability Modeling of Information Systems with Human Elements: A New Perspective”, *IEEE Transactions: Total Systems Reliability Symposium*, December, pp. 30-39.

Sun L., Srivastava R. P., and Mock T. (2006), “An Information Systems Security Risk Assessment Model under Dempster-Shafer Theory of Belief Functions”, *Journal of Management Information Systems,* Vol. 22, No. 4, pp. 109-142.

Wilkins E., and Lavington S. H. (2002), “Belief functions and the possible worlds paradigm. *Journal of Logic and Computation,* Vol. 12, No. 3, pp. 475-495.

Xu H., Hsia Y-T, and Smets P. (1993), “A Belief-Function based decision support system”. In, Heckerman, D.; and Mamdani, A., (eds.), *Proceedings of 9th Uncertainty in Artificial Intelligence*, pp. 535-542.

Yager R.R., Kacprzyk J., and Fedrizzi M. (1994), *Advances in the Dempster-Shafer Theory of Evidence*. New York, NY: John Wiley and Sons.

Yu S. and Neter J. (1973), “A Stochastic Model of the Internal Control System”, *Journal of Accounting Research,* Vol. 11, No. 2, pp. 273-295.

Zarley D., Hsia Y.-T., and Shafer G. (1988), “Evidential Reasoning using DELIEF”, *Proceedings of the National Conference of Artificial Intelligence*.

Figure 1: A Generic Evidential Reasoning Model for Sarbanes-Oxley Mandated Internal Control Assessment

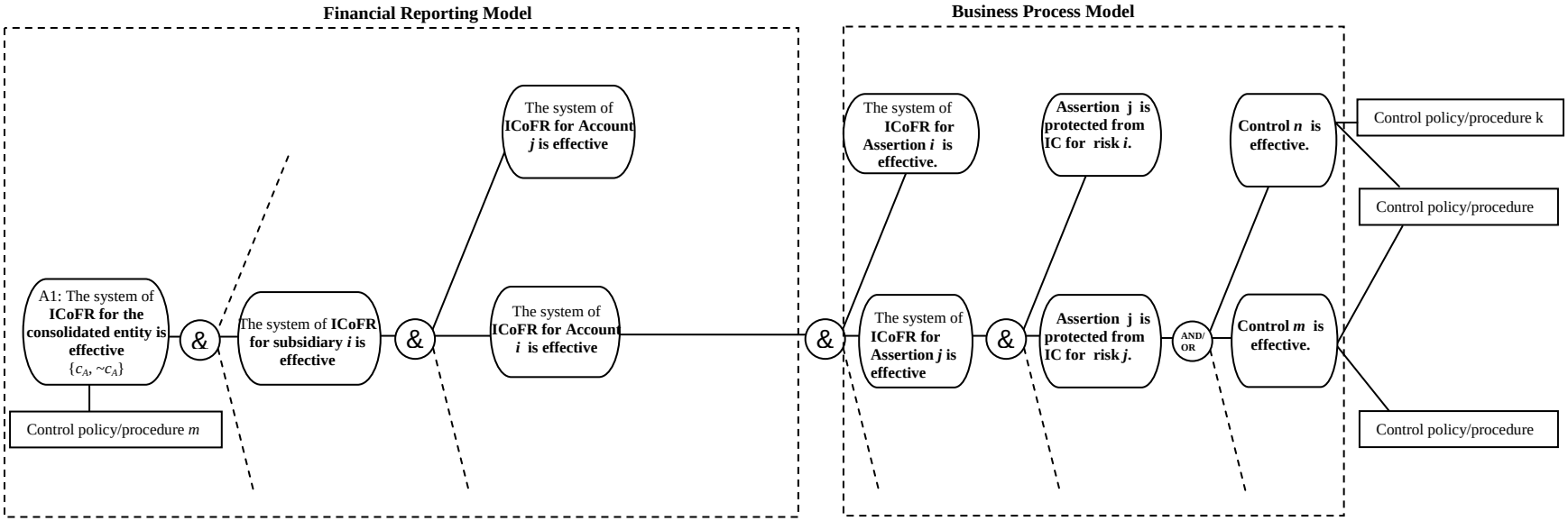


Figure 2: An Example of the Evidential Reasoning Model for the IC Effectiveness Evaluation under Auditing Standard No. 2

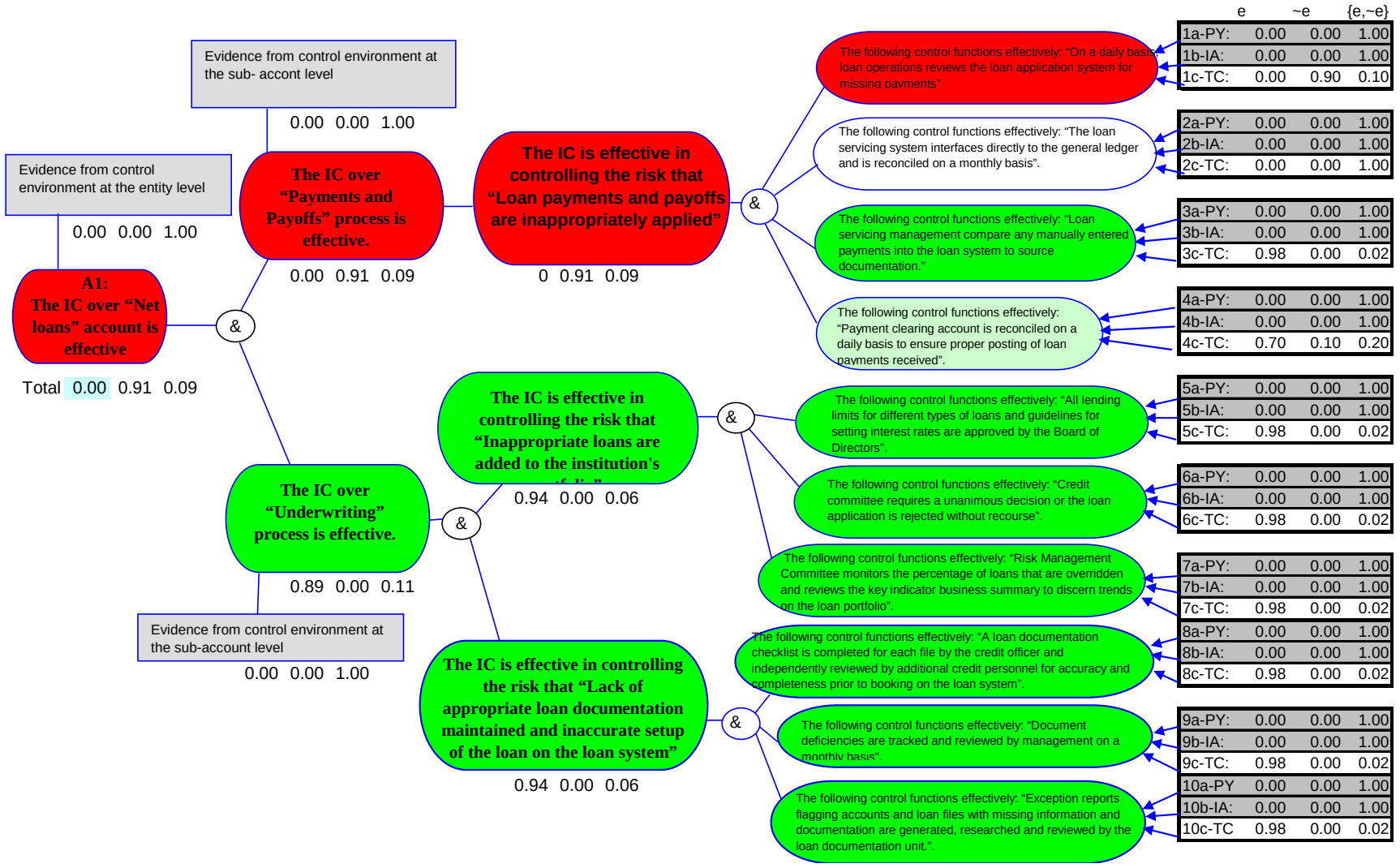
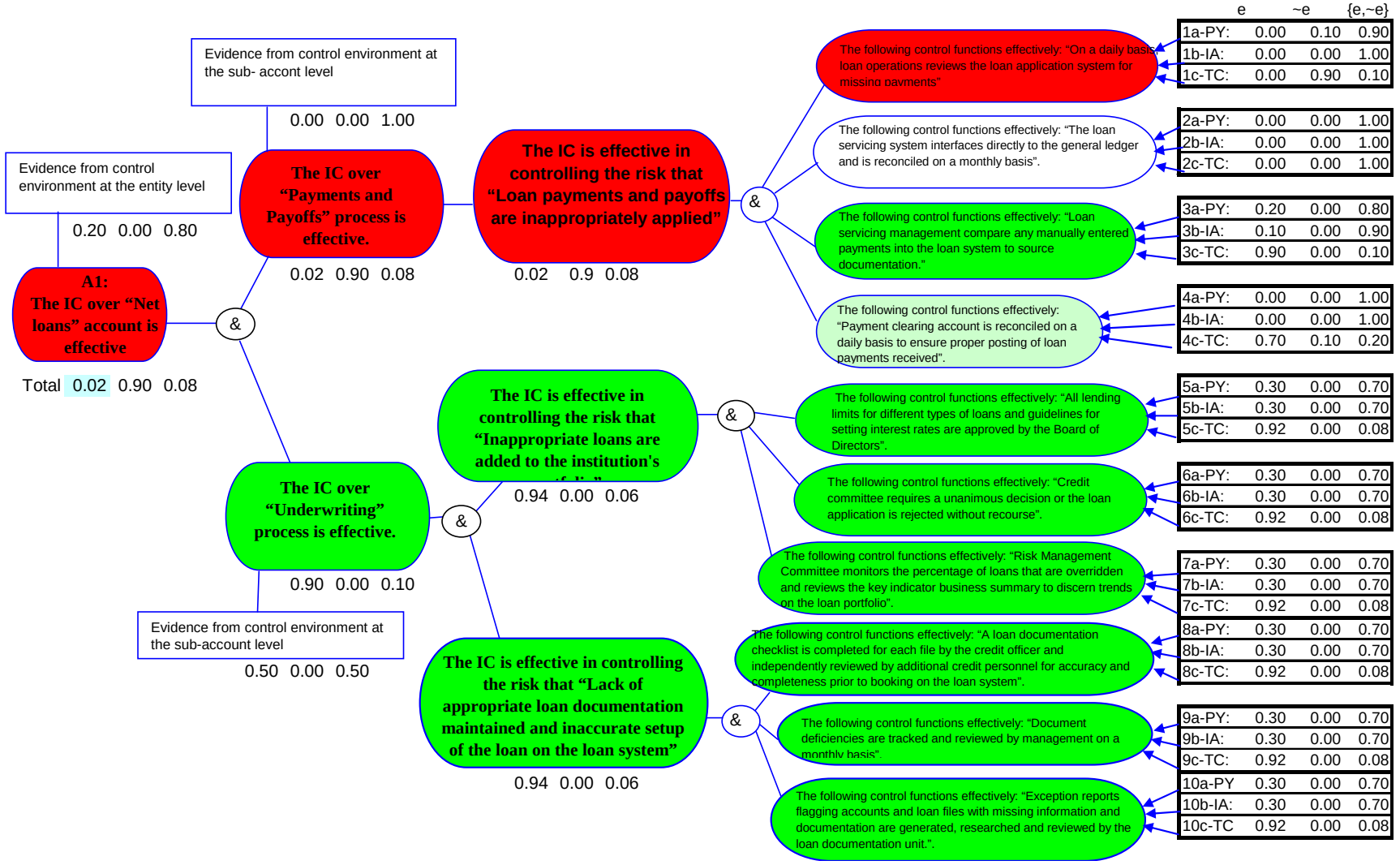


Figure 3: Evidential Reasoning Model for the IC Effectiveness Evaluation under Auditing Standard No. 5



Appendix A: Definitions of Basic Functions of Belief-Function Theory

The Dempster-Shafer (DS) theory of belief functions has its root in the mathematical theory of probability. Dempster's work during 1960's and Shafer's work during 1970's constitute the bulk of the foundational work on belief functions (see Shafer 1976 for details). However, the work done during 1990's by Shenoy and Shafer (e.g., see Shenoy and Shafer 1990) is what gave the computational power that was needed to propagate beliefs through a network of variables in a real world problem as done in the present paper. The basic difference between probability and belief functions is that how uncertainties are assigned to the state of nature in a problem. In probability framework, we assign uncertainty to each state of a mutually exclusive and collectively exhaustive set of states of nature. These uncertainties are known as probabilities and they all add to one. Under DS theory, as discussed next, uncertainties are assigned to all the singletons, all the subset of two elements, all the subsets of three elements, and so on to the entire set of elements. In principle, such a distribution is distribution of probability numbers over the super set of the mutually exclusive and collectively exhaustive set of states. There are three basic functions that are important for the current paper. We introduce them briefly along with the introduction to Dempster's rule of combination. Dempster's rule combination of independent items of evidence is similar to Bayes' rule of conditioning in probability theory. We elaborate this rule later in the section. Although Shafer's book *Mathematical Theory of Evidence* (19976) is still the classic reference on belief functions, interested readers are encouraged to see the following publications for recent references: Yager et al (1994), Srivastava and Mock (2002), Dempster et al (2008).

The Basic Probability Assignment Function (m-values)

The *basic probability assignment function* is one of the fundamental functions under DS theory. The following discussion elaborates the concept related to this function. Suppose we have a decision problem with n possible elements or states of nature forming a mutually exclusive and collectively exhaustive set represented by $\{a_1, a_2, a_3, \ldots a_n\}$. Call this entire set a frame represented by the symbol Θ. As mentioned earlier, in the belief-function framework, uncertainty is not only assigned to the single elements of the frame but also to all other proper subsets of the frame and to the entire frame Θ. These uncertainties are called *m-values* (Shafer 1976). Similar to probabilities, all these m-values add to one:

$$\sum_{A \subseteq \Theta} m(A) = 1,$$

where A represents all the subsets of the frame Θ, and $m(\varnothing)=0$, i.e., the m-value for the empty set is 0.

Belief Function

The belief function measures the overall belief in a state or combination of states based on the evidence gathered. Basically, the belief function for a subset of elements, say A of a frame Θ, is defined as the sum of all the m-values for the individual elements in the subset, A, and the m-values for any subsets contained in the subset, A. In terms of symbols:

$$Bel(A) = \sum_{A \supseteq B} m(B),$$

where B is any subset of A. For example, belief in the subset $\{a_1, a_2\}$ is: $Bel(\{a_1, a_2\}) = m(a_1) + m(a_2) + m(\{a_1, a_2\})$.

Plausibility Function

The plausibility function for a subset of elements A, of a frame Θ, is defined to be the maximum possible belief that could be assigned to A if all future evidence were in support of A.

Mathematically, plausibility is defined as:

$$Pl(A) = \sum_{A \cap B \neq \varnothing} m(B).$$

The plausibility function can also be defined in term of belief function as:

$$Pl(A) = 1 - Bel(\sim A).$$

Assuming A is an assertion that internal control is effective and ~A means that the internal control is not effective. The belief that the internal control is not effective is given by Bel(~A) where as the plausibility that the internal control is not effective is given by Pl(~A), which represents the *maximum* possible belief that the control is not effective. The plausibility in '~A', i.e., Pl(~A), in effect, measures the risk that the internal control is not effective. Srivastava and Shafer (1992) use such a definition of plausibility of material misstatement in the financial statements to be the audit risk.

Dempster's Rule of Combination

Dempster's rule is the fundamental rule for combining independent items of evidence in DS theory, similar to Bayes' rule in probability theory. For simplicity, let us illustrate Dempster's rule for only two independent items of evidence. Let us assume that m_1 and m_2 are the two sets of m-values obtained from the two independent items of evidence pertaining to a frame, Θ. The combined m-values (*basic probability assignment function*) for a subset A of frame Θ using Dempster's rule is given by:

$$m(A) = K^{-1} \Sigma\{m_1(B_1)m_2(B_2) | B_1 \cap B_2 = A, A \neq \varnothing\},$$

where $K = 1 - \Sigma\{m_1(B_1)m_2(B_2) | B_1 \cap B_2 = \varnothing\}$.

The constant K is known as renormalization constant. The second term in K arises because of the conflict between the two items of evidence. When K = 0, the two items of evidence are not combinable; they conflict each other completely.