A RISK SCORECARD FRAMEWORK FOR E-AUDITING IN INDIAN BANKING SECTOR

Partha Saha, Management Information Systems Group, Indian Institute of Management Calcutta, Calcutta, West Bengal, India, shree.partha.saha@gmail.com

Indranil Bose, Management Information Systems Group, Indian Institute of Management Calcutta, Calcutta, West Bengal, India, bose@iimcal.ac.in

Pradeep Ray, School of Information Systems, Technology and Management, The University of New South Wales, Sydney, Australia, p.ray@unsw.edu.au

Ambuj Mahanti, Management Information Systems Group, Indian Institute of Management Calcutta, Calcutta, West Bengal, India, am@iimcal.ac.in

Binay Bhushan Chakraborty, Finance and Control Group, Indian Institute of Management Calcutta, Calcutta, West Bengal, India, bbc@iimcal.ac.in

Abstract

Highly regulated sectors such as banking and insurance are confronted with a large body of regulations, standards and best practices for Governance, Risk Management and Compliance (GRC). In a developing country like India, the challenges before an auditor who is manually auditing a banking or insurance sector and who has to rely solely on individual experience, acumen, discretion and judgement to assess an organization's performance evaluation vis-a-vis various control requirements are daunting. The fundamental challenge lies in manually mapping and benchmarking banking processes and functionality with control requirements of GRC. Deviations often prove costly for the institution. To circumvent this difficulty in manual auditing process, in this paper we are proposing a novel application of ontologies in constructing an automated risk score card model in which knowledge is embedded at multiple hierarchical ontology layers that fosters scalability as well as modular designing principle. Many of the shortcomings of the manual auditing processes may be overcome by applying this scorecard model. This model as a DSS (Decision Support System) , facilitates the auditors to track fraudulent manipulations, lurking under colossal banking transactional/ operational data on a real time basis and arrive at unbiased automated estimation of performance of a bank.

Keywords: Risk Management, Compliance Auditing, Bank Risk Score Card, Ontology.

1 INTRODUCTION

Compliance auditing is a business process that is motivated by the industry requirement and regulatory practices to quantitatively measure (mis) alignment between organizational working practices and statutory regulatory policies and guidelines. The severity of the enforcement of regulatory guidelines resulted from a series of scams and corporate frauds especially in the US viz. Enron, HIH, Xerox, WorldCom etc. Various security surveys (E&Y Global Information Security Survey 2012) indicate highest premium placed upon any organization's information security triad CIA (Confidentiality, Integrity and Availability) by the industry as well as regulatory bodies. This scenario is more prevalent in the highly regulated and information rich sectors like banking, financial institutions and healthcare where large numbers of mandatory regulations (through internal business processes and IT controls) need to be rigorously complied with. Compliance auditing provides us a benchmark against which organizations' regulatory practices are quantitatively measured. It basically quantifies significant anomalies between regulatory standards and organizational process and practices .Stringent fines including potential jail terms are slapped on errant management for inability to impose sufficient checks and controls on veracity of publicly available reports (which measure financial health of the organizations) and thereby jeopardizing stakeholders' interest.

In this paper we are giving a brief description of ontology based multi-agent model for e-auditing in the banking sector. Ontology, which traced its root in ancient philosophical discourse, is defined as a "formal specification of a shared conceptualization" (Borst, 1997). Ontology formally contains a quadruple set (of concepts, relations, axioms and instances) and may also be graphically represented as a directed graph with tuple (nodes, nodes contents and arrows) representing (concepts, instances and relationships) respectively. In this paper we have designed a multi-layered ontology based audit scorecard in which knowledge is embedded at different hierarchical ontology layer that fosters scalability as well as modular designing principle. The research challenge we are trying to address is how the ontology may be used in structuring and implementation of the automated risk score card model. We will also try to understand how this audit framework helps discover patterns of anomalies in banking process. However the implementation aspects of this model (multi agent based architecture) may not be pursued due to size restriction of the paper.

The paper is organized as follows. In the second section we give a brief introduction of information system audit, including its scope and methodology. In the third section we are examining relevant literature in compliance auditing, information security and ontology based models in different domains while in the fourth section we briefly describe significance of our research. In the fifth section one real life case study related to banking audit is presented. In the sixth section ontology based multi-agent model for e-auditing in the banking sector is illustrated while in the seventh section a framework for e-banking audit scorecard is elucidated. In the eighth section we describe in detail the credit management of a bank operating in SME (Small and Medium Enterprise) sector, the deviant activities of the agents and their measurement. In section nine limitations of the present paper as well as future scope is discussed. The paper concludes with section ten.

2 FOUNDATIONS OF INFORMATION SYSTEM AUDIT

In this section we discuss some of the core issues of auditing including audit scope and methodology in a succinct manner. The scope and methodology are generic enough even though they have been applying here in the specific case of banking audit.

2.1 Scope of IS Audit:

The IS audit scope encompasses a wide gamut of processes and activities including collection and evaluation of evidence/information to determine safeguarding of asset and its safety, security, confidentiality, integrity, availability of data, achievement of organizational goals, optimum utilization

of resources including human resources and its training, IS processes , its deployment preparedness, monitoring and adequacy.

2.2 **Information Systems Audit Methodology**

The IS auditing procedures involve manual auditing , computer assisted procedures , fully automated auditing procedures (using Computer Assisted Audit Tools called CAATs) or a mixture of these techniques. An auditor may conveniently switch from limited random and statistical sampling techniques to automated CAATs based auditing which verifies every record. For convenience and effectiveness the whole auditing process is broadly divided into five major segments viz. (a) Planning IS Audit (b) Tests of Controls (c) Tests of Transactions (d) Tests of Balances (e) Completion of Audit

2.2.1 Planning IS audit

Planning being the first step in the auditing requires a thorough understanding of auditee's organization/office/department and departmental process. In audit process there are hosts of issues to be considered viz. collecting background information about human resources (skill set, aptitudes, key resource persons, system ownership, hierarchical patterns, and appropriate staff assignment), transactional processes as well as identifying risks, detailed analysis, testing internal controls(through review of previous audit reports, interview and interaction with management and key resource personnel, observing critical activities and review of IS documentation), testing and its impacts.

2.2.2 Tests of Controls

Internal control consists of testing of management controls and application controls and both need to be tested separately to evaluate reliability, lacunae, weakness and vulnerability . During this phase of IS audit, Internal Controls are tested to evaluate whether they operate effectively. The objective is to evaluate the reliability of the controls and find out weaknesses of the controls for meeting the IS audit objectives. IS auditor is required to make recommendations to rectify the weaknesses, observed during the course of an IS audit.

2.2.3 Tests of Transactions:

Test of transaction is used to check database integrity through various levels of scrutiny (like tracing of journal entries, testing of computational accuracy, evidence gathering through transactional logs etc.). CAATs are normally deployed to perform these types of transaction testing.

2.2.4 Tests of Balances:

This type of audit testing quantitatively calculate the extent of losses when IS fails to achieve some of its stated goals viz. protection of assets, data integrity, effectiveness and efficiency of systems. Various tests are performed for verification of data integrity and protection of assets (receivable confirmation, inventory verification and recalculation of depreciation on the fixed assets) as well as measuring effectiveness and efficiency of systems (which may require specialized audit software).

2.2.5 Completion of audit

In this last phase of auditing auditors are required to discuss with the appropriate authorities the gist of their findings, analysis and preliminary recommendations in a structured format . The exit meeting should document and include the auditee's comments and questions concerning the preliminary IS audit questionnaires and recommendations as prepared in a format called issue summary sheet. Final version of the audit report (which is composed of audit objectives, general approach, critical findings and datasheet to support them, potential consequence and recommendations) should be submitted to management after reconciling auditee's response.

3 LITERATURE SURVEY AND RELATED WORKS

With the globalization of economy, stakeholders' pressure on the corporate sector to conform to ever increasing demands of regulations , which are meant to satisfy information integrity and confidentiality of the organization, has considerably increased. This is also true for business continuity in a networked environment (Price Waterhouse Cooper , 2006 ; AusCERT, 2006). Various security surveys also emphasize these mandatory nature of compliance regulations in light of various security scams around the financial world(Ernst & Young 2012). Over abundance of country specific rules, regulations(Basel III, HIPPA , Gramm Leach Bliley), security standards and best practices (CobiT, ISO 17799, ITIL, Baseline Protection Manual (BSI))and mandatory cost of compliance to meet those regulations, exert an enormous burden on organizations' manpower and scare resources (Parry 2004; Ashbaugh-Skaife and Collins 2008; Volonino, Gessner , and Kermis 2004). The standard of good practices are designed to maintain sanctity of corporate governance as well as protection of assets and valuable resources (Saha, Pramesswaran , Ray and Mahanti 2011). Inability to comply with various regulations attracts huge penalties from the regulators (Parry 2004). US based companies alone spend around $30 billion on corporate governance, risk management and compliance related solutions and over the years this expenditure continues to increase sharply (Hagerty and Kraus 2009; OpenPages 2009).Implementation of labour intensive, continuous and iterative nature of compliance auditing process require alignment of organizational process and internal business/IT control(Wong, Yip , Ray and Paramesh 2008). Hence the need for dedicated information systems to significantly cope and manage compliance with newer regulations cannot be overemphasized (Volonino, Gessner and Kermis. 2004; Fisher 2007; Wiesche, Schermann, Krcmar 2011). Automation in compliance auditing process may therefore be inevitable given different organizations' unique systems, technology, domain, risk assessment country and environment, variety of requirements with different emphasis as well (Abdullah, Induslka and Shazia 2009; Wong, Yip , Ray and Paramesh 2006; Heiser 2010). There is also scope for valuable knowledge (explicit as well as implicit) sharing and reuse (Wiesche, Schermann and Krcmar 2011;Wong, Yip , Ray and Paramesh 2008; Teubner and Feller 2008).

Existing computer-assisted compliance management solutions only address a relatively small subset of compliance management solutions viz. configuration and patch management, license management and change management which are also vendor/technology specific.(Lau, Law and Wiederhold 2005; Managesoft 2007; Symantec. 2006).

Our approach in this paper (Ontology based Multi Agent System) plays a pivotal role in compliance auditing. Ontology, a branch in metaphysics, is defined as "*a formal specification of a shared conceptualization of a domain"*(Borst 1997). Ontology captures implicit and explicit knowledge which can be shared, reused and consumed by autonomous agent (Gruninger and Lee 2002). Ontology provides knowledge base to Multi Agent System for various system operations including network management, security solutions, legal, forensic and financial applications, software engineering and healthcare. At the University of Edinburgh (UE) ontology and computational framework is being designed that supports fraud detection, forensics analysis and legal reasoning (Leary, Vandenberghe and Zeleznikow 2003). The FF POIROT project in Belgium attempts to build a detailed ontology of European Law and financial fraud (Jamieson 2003; FF POIROT).Here in our paper we are trying to develop multilayer Ontology architecture across whole agent platform for e-auditing which ensures operational activities complying with rules and regulations.

4 SIGNIFICANCE OF RESEARCH

In this section we discuss significance of our research in light of auditing which is specific to Indian banking sector. In Section 3.1 we discuss certain issues which are unique to Indian banking sector while in Section 3.2 we summarize some problems pertaining to manual auditing. In Section 3.3 uniqueness of our approach (Ontology Based Multi Agent System (OBMAS)) while designing an automated audit score card and how it may transform manual auditing, is elucidated.

4.1 Problems specific to Auditing in Indian Banking Sector

With the liberalization of Indian economy, ubiquitous penetration of ICT (Information and Communication Technology) both in the asset as well as liability side of banking, finance and insurance sector has interspersed with this sector's explosive growth (average18% which has far outstripped India's average GDP growth (7%)) in the last couple of decades. Existence of multiple delivery channels, wholesale and retail payment/settlement systems have augmented turnover of financial and commercial transactions. These facilities also brought forth host of formidable challenges for the banking sector as well as for the auditor engaged in auditing the bank. These multifarious challenges for the auditor relate to, inter alia, co-existence of multiple controls for legacy and automated systems in the Indian banks, technology complexities and obsolescence, frequent changes in legal and regulatory requirements (including cyber laws), dependence on outsourcing and vendor related concentration risks, inadequate segregation of duties, external and internal threats from employees, fraudulent appropriation of loan funds through dubious means (forged documentation, overvaluation/non-existence of collaterals, identity theft, misappropriation of accounts, misuse of power of attorney et al.) and so forth. Hence the task of an auditor, (who is manually auditing an Indian bank and facing some/all of the challenges mentioned above) becomes extremely unenviable. Hence the importance of an Automated Audit Score Card for an auditor as a DSS (Decision Support System) tool cannot be overemphasized.

4.2 Shortcomings associated with conventional manual auditing process

The conventional manual auditing process, that is in force in banking and other finance domain in India (as well as in most of the other developin countries) suffers from some major lacunae viz. (i) Auditing being a long, tedious, manual and labour intensive process (for the auditor as well as for the auditee), it is prone towards being subjective , biased and full of human error (ii) Auditing being a human driven activity, interpersonal relationships between auditor and auditee as well as various extraneous factors (subjective as well as objective) play a significant role in determining audit output, comments and recommendations (iii) Auditing being a long and elaborate process (that span across multiple domain, departments, multiple interactions and iterations) it becomes very difficult in maintaining uniformity, accuracy and consistency of results and recommendations over a period of time while dealing with human factors (iv)Audit , being highly labour intensive activity, is also a very costly affair and hence its efficiency (ratio between accrued benefit and cost incurred) often becomes questionable .

4.3 Ontology Based Multi Agent System (OBMAS) for designing e-Auditing Score Card

In this paper a new approach (viz. Ontology Based Multi Agent System (OBMAS)) is proposed to overcome the shortcomings and limitations of the prevailing manual auditing , by applying techniques from diverse fields including ontology, agent based system and semantic based rules. This new approach displays some salient features as follows: (i) total knowledgebase captured in the compliance auditing process, is systematically distributed in a multi layered ontology framework where knowledge entities are formally defined in a parent-child relationship where lower ontologies inherit all the attributes of their parent (upper) ontologies. (ii) Banking processes are explicitly defined in terms of contexts, levels of abstraction, behaviors, mechanisms, agents and situations (iii) Software agents may be used to perform intelligent processing / reasoning with various ontological layers through logic based interface (iv) During automated auditing process, software agents may cooperatively, recognize certain fraudulent patterns and track fraudulent behaviors (through explicit ontology based dialog mechanism) of the stakeholders (including customers and employees) (v) through modification/alterations of various modules within a specific ontological layer different banking auditing scenarios can be constructed differing on various levels of specification, granularity and abstraction (vi) Ontology plans and protocols may be systematically and dynamically altered and cooperatively derived and executed to make it flexible and reusable across multiple applications.

By adopting OBMAS methodology manual compliance auditing may be transformed into followings:

- Through computerized processing *Compliance Checklist Items* may be generated (semi)automatically
- Similarly the methodology (through Q&A process of compliance verification) can be (semi)automatically performed via logical interface and reasoning
- Compliance results become relatively uniform, predictable and traceable through this (semi)automation procedure
- As through multi layered ontology construction embedded banking knowledgebase and auditing procedures become explicitly, systematically, formally and mechanically defined adaptability and reusability across heterogeneous domains may become feasible.
- Resulting benefit accrued are increased efficiency, consistency, cost reduction, accuracy, reusability and repeatability of compliance auditing process.
- One major challenge exists in relation towards our ontology based semantic approach towards compliance auditing in the banking sector viz. missing, unknown, ambiguous and misleading data(especially related to fraudulent cases). This fault tolerant capability towards deceptive and unpredictable quality of data in the real world banking sector imposes a critical challenge towards the rule based semantic approach which requires information and knowledge in explicitly captured format. This hard problem (which calls for human intervention for resolution of problems under imprecise circumstances) is handled through fuzzy logic and weighted fuzzy production rules to implement approximation in reasoning (while handling missing/ambiguous/imprecise knowledge/concepts/instances/ relationship) during construction of semantic based compliance auditing.

5 IMPORATANT CASE STUDY (DETECTED WHILE AUDITING IN THE BANKING SECTOR)

In this section we will briefly summarize a particular case where various irregularities pertaining to banking operations (loan processing, sanctioning, and term-deposit et al.) were finally discovered during audit/special audit sessions at the bank. Fraudulent documentations, over valuation/non-existent collaterals, misuse of power of attorney, identity theft and account takeover are some of the modus operandi used by the perpetrators, which were detected during auditing. This particular case is taken from a portfolio of around 700 cases where data have been systematically collected from various secondary sources e.g. banks (private, public, co-operative, rural, foreign banks) , audit /chartered accountant firms etc of a particular country. Considerable efforts have been made to deliberately mask the identity of concerned banks, people and places to immunize the data sources. Monetary instruments have been converted from local currency to USD (converted to nearest integer value) to facilitate uniform understanding. In Section 7.5 we will show how our proposed audit scorecard model, if implemented, might have prevented this type of fraud.

Case Study. (Obtaining Overdraft through mortgage of the property)

This case was referred to internal audit when an advance overdraft of $40692 was sanctioned by the concerned Bank Manager (BM) under trader incentive scheme in the first quarter of 2010. But the irregularity came to light two years later only in the first quarter of 2012. The facility was collaterally secured by EM of property purportedly owned by the guarantors. Internal audit revealed that Inland Letter for confirmation, Letter of Guarantee as well as some other important documents were not held at the branch. It was further revealed that the bank is in possession of the Xerox copies of the title deed. Some of the mandatory Standard Operating Procedures (SOP) , supposed to be strictly followed by bank officials were also not adhered to while disbursing the loan. Finally the case was referred to the police for criminal proceedings.

6 ONTOLOGY BASED MULTI-AGENT MODEL FOR E-AUDITING IN THE BANKING SECTOR

In this section we propose to build a multi-layered ontology to be used by computational agents for the purpose of e-Auditing a bank. Using ontology as the core of their functional eco-system, the agents will interact in a co-operative manner to evaluate the audit risk score card of the concerned bank. Audit risk score card is a quantitative risk measurement tool to calculate the risk rating of a bank where higher score implies higher risk for the bank .The agents will use the structured format of query processing tools and dialogue management techniques (to be described in the next section) to calculate the aforementioned audit risk score card. The proposed framework called OBMAS (Ontology Based Multi Agent System) may be elucidated as follows.

The basic paradigm underlying the construction of OBMAS architecture is the existence of hierarchical structures which accommodate various ontology layers. These ontology layers capture concepts/knowledge which is monotonically more abstract/generic and particular/specific than concepts/knowledge hosted in the immediate lower/higher hierarchical layers respectively. Concepts/knowledge embedded at the lower level ontologies may be expressed in terms of higher and/or equivalent concepts/knowledge level. This architecture, which fosters modularization and scalability, may be composed of following four abstraction layers viz. (i) Foundational Layer (ii) Domain Layer (iii) Topical Layer (iv) Application Layer

6.1 Foundational Layer

This top layer contains ontologies which incorporate basic ideas and concepts. These ideas/concepts are generic in nature. They are fundamental building blocks (e.g. arithmetic operations, processes which are applicable throughout multiple domains) upon which other ontologies are created. SUMO (Suggested Upper Merged Ontology), created by the IEEE Standard Upper Ontology Working Group, is a particularly apt example of top tier ontology

6.2 Domain Layer

This layer incorporates ontologies that contain concepts/ideas, embedded in the parent domain(s). In our present application, audit scorecard calculation of e-banking sector may incorporate domain level concepts from such diverse domains viz. Information security, banking rules, application, operations etc. Here we need to develop/reuse/expand existing domain ontologies to capture the required framework for audit score calculation.

6.3 Topical Layer

This layer hosts ontologies related to banking audit scorecard database and audit scorecard calculation. The former ontology (audit scorecard database) captures distinct concepts related to scorecard development (banking operations, applications, revenue leakage, security, disaster recovery etc) which are used by the latter (audit scorecard calculation ontology) to calculate the audit risk score S. On a scale of 10, the audit scorecard S calculates the particular audit risk score of a bank by a parametric equation to be described later. Lower the score on the S scale, higher the scope of satisfactory report, to be obtained by the bank. Specialized domain related concepts (e.g. information security, banking rules, regulation and applications etc.) are captured in this layer. This layer also segregates different aspects of risk management, such as risk impact and risk weight distribution of various banking activities and operations captured in the audit scorecard database ontology.

6.4 Application Layer

This layer accommodates ontologies which are tightly integrated with Information System Risk Scorecard evaluation procedure. This ontology is based on Audit Risk Scorecard Calculation Ontology

described in the Topical layer. The risk score S, based on a scale of 10 for the particular bank (which is calculated in the aforementioned ontology), is evaluated here and the bank is placed in one of the four categories based on the S score. In general, lower the score of the bank on the S scale, higher is the likelihood of its audit compliance.

The hierarchical ontology development model is elucidated in Figure 1. As described earlier, the components of this model are segregated into four distinct layers (Foundational, Domain, Topical and Application). Lower level concepts derive their meaning and applicability in terms of equivalent or higher level concepts (e.g. at the application level the ontological concept "evaluation" is expressed in terms of attributes like "equation" and "addition" (at the foundational level ontology) and "criteria X1" and "criteria X2" (at the topical level ontology). The ontological inheritance of attributes is indicated by the cross-reference links .

7 CONSTRUCTION AND EVALUATION OF E-BANKING AUDIT SCORECARD

In this section we described the construction of audit risk scorecard framework to be used for auditing a bank. Auditing a bank requires measuring risk scores to be quantitatively calculated in several sectors of the banking operations. These sectors include banking operations, revenue leakage, application, security, disaster recovery, application level, physical and environmental control, data integrity, miscellaneous etc. Risk scores of different components in each of these sectors need to be quantitatively calculated individually and added to arrive at the overall audit risk score of the bank. Risk score of an individual component is measured by multiplying risk impact and risk weight of that component. While the risk impact depicts the severity of the risk, risk weight measures risk on a scale of 4(insignificant=0, low=1, medium=2 and high=3). Audit Risk Score S captures the notion of risks faced by the bank. We now apply ontological concepts for the construction of audit risk scorecard framework. The scorecard framework is shown in Figure 1. While describing the model in Figure 1 we describe it in a bottom up manner i.e. starting from Principal Application Layer.

7.1 Ontologies in Principal Application Layer (Audit Scorecard Evaluation)

In this layer the evaluation ontology segregates and ranks the audit of the bank according to the value of audit risk scorecard S. Principal Application Layer ontology uses results of two upper layer ontologies viz. Audit Scorecard Calculation ontology (at Topical Layer which calculates risk score S) and Arithmetic ontology (at Foundation Layer which uses generic concepts like addition, multiplication, subtraction etc.). As stated earlier, on a 10 point scale, lower the value of S, higher is the chance for the bank to get a compliance report from auditor. In this regard four cases (corresponding to different values of S) may arise depending upon the performance of the bank during auditing. Different values of risk score S and corresponding audit remarks are shown in Table 1. Major corrective measures and huge penalties may be imposed on the bank when risk score S >6 (poor performance or negative remark). Minor or no correction may be required when S≤6. When risk score exceeds 7.5 the auditor may give negative report which might call for drastic steps including closure or heavy penalty indicating performance of the bank is below standard level of expectation.

Sl. No.	S Value	Audit Remark
1.	S≤4.5	Satisfactory
2.	6 ≥S > 4.5	Needs Improvement
3.	7.5 ≥S >6	Poor Performance
4.	10≥S > 7.5	Negative Reject

Table 1. Audit Score S vs. Audit Remarks

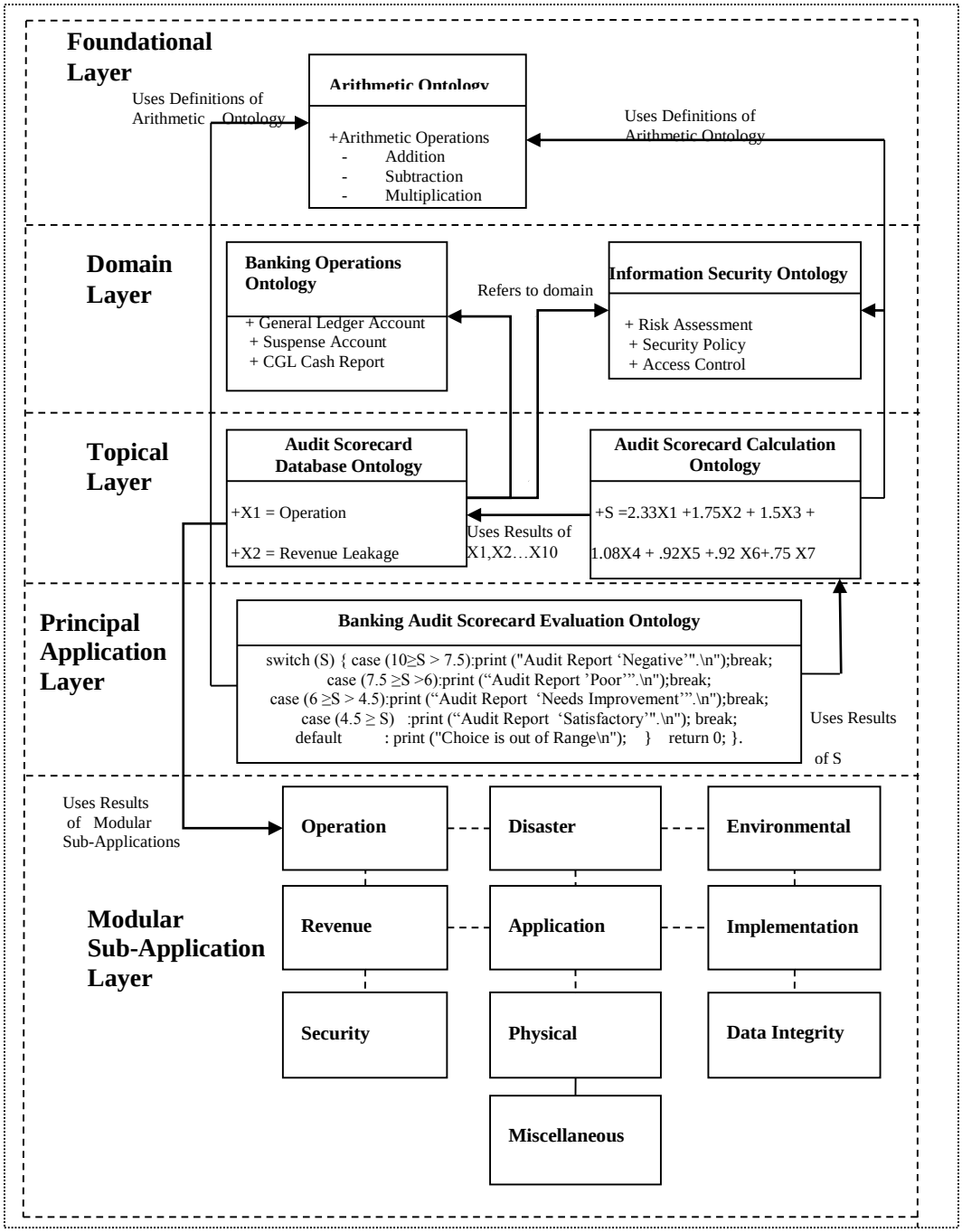

Figure 1. Ontology Hierarchy for Banking Audit Scorecard (Detailed Overview)

7.2 Ontologies in Topical Layer (Scorecard Database and Scorecard Calculation)

In this layer the two major ontologies (Audit Scorecard Calculation Ontology and Audit Scorecard Database Ontology) exist who cooperate with each other in calculating the credit score S. Audit Scorecard Database Ontology contains the components used by the Audit Scorecard Calculation Ontology to arrive at the audit score S of the bank. Each of these components represented by X1(Operational Component), X2(Revenue Leakage Component) to X10 (Miscellaneous Component) represents various aspects of banking operations and corresponding individual component of risk score

indicates how risky these aspects are as determined by the auditor (whether satisfactory, needs improvement, poor performance or negative reject).

Sl. No.	Variables	Variable Meanings	Variable Component X's Maximum Risk Score(MRS= $X(j) = \sum_{i=1}^{n} \sum(\text{Risk Impact } (\text{RIi}) \text{ x Maximum Risk Weight}(\text{MRWi}))$ where there are n Sub-Components of Variable Component X; hence Sub-Component i varies from 1 to n)	Variable Coefficient (=Maximum Risk Score× 10)/Total Risk Score))
1.	X1	Operational Component	88	840/360=2.33
2 .	X2	Revenue Leakage Component	63	630/360=1.75
3.	X3	Security Component	50	540/360=1.5
4.	X4	Disaster Recovery Component	36	390/360=1.08
5.	X5	Application Level Component	33	330/360=0.92
6.	X6	Physical Component	33	330/360=0.92
7.	X7	Environmental Component	30	270/360=0.75
8.	X8	Implementation Component	6	60/360=0.17
9.	X9	Data Integrity Component	6	60/360=0.17
10.	X10	Miscellaneous Component	15	150/360=0.41
Total			360	10

Table 2. Variable Components, Meanings and Coefficients

The scorecard model is described by the equation 1 and 2 while XI, X2…X10 are the variables which are described in Table 2

$$S = 2.33X1 + 1.75X2 + 1.5X3 + 1.08X4 + .92X5 + .92X6 + .75X7 + .17X8 + .17X9 + .41X10 \quad (1)$$

$$X(j) = \sum_{i=1}^{n} (\text{RIi x RWi}) \quad \text{where } 1 \leq j \leq 10,\ 1 \leq \text{RIi} \leq 3 \text{ and } 0 \leq \text{RWi} \leq 3,\ 2 \leq n \leq 20 \quad (2)$$

Each of the variable component of X(j) (X1, X2, X3… etc) has number of sub-components i($1 \leq i \leq n$). Maximum number of Sub-component in our model is 20 and each of these Sub-components has specific risk score. Risk score of each variable component i is calculated by multiplying Risk Impact (RIi) ($1 \leq \text{RIi} \leq 3$) with Risk Weight RWi ($0 \leq \text{RWi} \leq 3$) of all the sub-components i($1 \leq i \leq n$) of that particular component X(j) and then summing them up. In this way the operational and revenue leakage component has total risk score 84 and 63 respectively. Each variable X(j)'s coefficient is calculated by dividing 10

times Maximum Risk Score by Total Risk Score . In this way we find the coefficient of X1 as 840/360=2.33. In the next sub-section . we will restrict ourselves to show how the risk score is calculated for the second variable components viz. Revenue Leakage Component (X2) only . Due to lack of space other nine components (operational, security etc) , with their ingredient sub components , cannot be described in detail

7.2.1 Calculation of Normalized Risk Score for Revenue Leakage Component (X2) of Banking Operations

In this subsection we will be dealing with risk score calculation of another particular variable component viz. X2 (Revenue Leakage Component) which is explained in Table 3. The normalized risk score of 6.67 may attract "Poor Performance" tag from the auditor (vide Table 1) prompting scrutiny.

Sl. No.	Critical Banking Transactional Process (Exceptional Reports have Risk Impacts)	Risk Impact (RI)	Risk Weight (RW) (Extracted from Audit Observations)				Risk Score = RI×RW
			NA	Low	Moderate	High	
			0	1	2	3	
1.	Diligent Pre-Sanction Process Summary Sheet for Borrowers/ Guarantors through KYC (Know Your Customers)	1			•		2
2.	Due Diligence undertaken while verifying Documents/Financials submitted by Borrowers	3				•	9
3.	Veryfying daily exceptional reports generations , checking and signing by the Branch Head	2		•			2
4.	Counter Checking if Pledged Properties are already mortgaged to other Bank / Financial Institutions prior to Loan Sanction	3			•		6
5.	If more than one independent verifications of pledged Properties are undertaken prior to Loan Sanction	3		•			3
6.	Due Diligence for verification of Credit worthiness of outside agencies undertaken prior to engagement	2			•		4
7.	Antecedent of Borrower's Credit History appraisal prior to Loan Sanctioning	2				•	6
8.	Penal Provision against Bank's Empanelled Advocate /Valuer/Consultant for professional improprieties	1			•		2
9.	Provision of cross checking of two or more Advocate /Valuer/Consultant's opinion regarding high value portfolios and identifying discrepancies	2			•		4

10.	Provision of close monitoring of loan accounts with irregular reimbursement (sign of incipient sickness of NPA (Non Performing Asset))	2			•		4
	Normalized Risk Score =X2=Total Risk Score/Maximum Risk Score [Maximum Risk Score $= \sum_{i=1}^{9} (RIi \times MRWi) = \sum_{i=1}^{9} (RIi \times 3) = 21 \times 3 = 63$]						42/63= .667

Table 3. Risk Score Calculation for Revenue Leakage

7.3 Ontologies in Domain Layer (Banking Operations and Information Security)

In this layer various banking operations and activities (suspense account, clearing inward-outward, CGL etc.) as well as information security (risk assessment, security policy, access control etc.) concepts are precisely defined. Topical layer ontologies use these concepts whenever required. By changing these rules and knowledgebase in this layer different applications may be implemented.

7.4 Ontologies in Foundational Layer (Arithmetic Operations and Processes)

In this layer ontologies belonging to the most generic nature (arithmetic ontology, process) may be defined. All other layers are below this foundational layer and use the concepts defined here.

7.5 Evaluation of e-Banking Audit Scorecard (vis-a-vis Bank Case Study)

In Section 3.1 we briefly described what difficulties are being faced by the auditors while auditing an average Indian bank and also in Section 5 we describe a particular case study in Indian banking sector where loan was sanctioned without proper verification of documents as well as without following SOP (Standard Operating Procedure) of the bank. In this subsection we will go deep into the current state of affairs in manual auditing in Indian banks, limitations prevalent into the system and how the audit score card as DSS (Decision Support System) may help plug the gap at some of the loopholes that exist in the current highly unstructured auditing ecosystem.

The basic paradigm change that the audit score card is designed to introduce is by changing auditing from reactive to proactive DSS tool. From a recent survey (Deloitte 2012) it is revealed that 70% of cases took more than 6 months and 40% of cases take more than one year to be detected it and hence it is no surprise that over 60% of cases less than 25% of the fraudulent transaction may be recovered (Deloitte 2012). Similar pattern is easily discernible from analysis of our portfolio of banking case studies. It is therefore hardly surprising that by the time anomalies are detected, the perpetrators have made good use of the time interval and nothing much may be done to retrieve the situation.

Our automated audit score card tries to address this situation by incorporating monitoring and recommendation to the bankers and auditor(s) on ten important banking aspects (Operation, Revenue Leakage, Security, Disaster Recovery, Application Level, Physical, Environmental, Implementation, Data Integrity, Miscellaneous) on a real time bases (vide Table 2). Each of the 10 components will mine through humongous amount of banking transactional/ operational data and identify hidden tangled relationship as well as potential red flags. This will help identify auditors and banks to identify potential fraudulent transaction before they explode in months or years down the line. As stated earlier in Section 7.2, due to lack of space only one of the ten components (Revenue Leakage) could be illustrated in detail in Section 7.2.1.

Now let us see how the problems encountered in case study could have been averted had the audit score card been used. There are three major lacunae encountered in the case (i) the SOP (Standard Operating

Procedure) was not followed while disbursing the loan (ii) Loan was sanctioned without procuring major documents like Title Deed, Letter of Guarantee, Letter of Confirmation etc. (iii) the irregularities in the manual procedures were discovered after two years. Again as we are not able to show effectiveness of all nine other components of audit score card, let us see how the Revenue Leakage Component (as shown in Table 3) alone could forestall most of the loopholes in the case study. By digitizing pre sanction process of borrowers/guarantors, verifying documents, financials submitted by borrowers, by exchanging network with other banks if same collateral is mortgaged to other banks, antecedent of borrower's credit history prior to loan sanction, strict monitoring of empanelled lawyers and cross verifying their opinions, automatic monitoring of loan etc the major component of irregularity in $40692 loan sanction (without proper verification of relevant document) could have been easily avoided. By digitization of relevant information, simultaneous alerts at multiple levels of loan sanctioning authorities (exception handling reports in row 3 of table 3) can be achieved enhancing chance of detection and rectification (which did not happen at manual process of loan sanctioning where data often moves in a bottom-up manner and can be suppressed/hidden by lower level authorities) . This automated audit score card could have prevented the time lag of two years (between loan sanction and anomaly detection) easily and the lacunae might have been detected/prevented in a couple of days rather than two years. Finally the non-application of SOP might have been detected by other nine components (which were not discussed) of the audit score card and could have made its way into exception report. As of now an auditor is under immense time pressure to sift through huge banking data in India, the audit scorecard may go a long way towards preventing fraud as well as a smart DSS for the auditors.

8 EVALUATION OF CREDIT MANAGEMENT PROCESS FOR REVENUE LEAKAGE COMPONENT IN E-BANKING AUDIT SCORECARD

In this section we describe the underlying process which goes behind the construction of audit risk scorecard framework to be used for auditing a bank. Here we describe the credit management process of a bank in great detail. We describe the credit management flow, the prescribed activities of the concerning agents, their deviant actions and the technique to measure the deviant activities. There are two types of deviant activities by the concerning agents viz. policy based violation and entity based violations. In most of the real life cases both these types of violations occur intermittently. To measure those types of violations two types of models are used viz. similarity measurement and impact function. The former measures the deviation between two events on the point of inception and try to predict the probabilistic future (hence more efficient but less) while the latter is very predictable because it is measured on the point of actual occurrence. Hence it is a tradeoff between efficiency/automation vs. predictability/accuracy. Finally we take up the case of non-existent/overvalued collateral in greater detail and try to correlate how the various deviant events play an important role in determining risk impact and risk score (which is very important from auditing point of view).in Table 3 of the previous section.

8.1 Credit Management in SME (Small and Medium Enterprise) Sector in Bank

Auditing is a process which examines, measures and validates whether a set of temporal events, which were executed as part of approved organizational activities (which take place over a period of time), is in conformity with "framework of certain standard reference parameters". Hence "compliance or conformity to regulations, obligations & standards" of specific organizational activities become hallmark of auditing. In other words auditing quantitatively measures the lacunae or deviations between prescribed and actual practices.

Figure 2 summarizes the credit management and process deviation ontology of a bank operating in a SME (Small and Medium Enterprise) sector.

Figure 2. Credit Management and Process Deviation Ontology of a Bank

Here as part of auditing, we are minutely examining the revenue leakage component of auditing a bank. Bank's credit management (credit application, credit appraisal, credit sanction, credit disbursement, credit repayment and credit monitoring) is centrally and pivotally linked to the revenue leakage component of the bank. In this case we are concerned with the credit management vis-à-vis SME (Small and Medium Enterprise) Sector.

Credit application process consists of prospective applicant enquiring, soliciting, matching requirements, selecting the product, filling out the relevant forms and submitting relevant documents. This process involves interactions between loan applicants and LSO (Loan Sourcing Officer) and other banking staffs at various hierarchical levels.

Credit appraisal mainly concerns verifying applicant's credit history, calculating applicant's credit score as well as scrutinizing and validating the applicant's submitted documents. This part is extremely critical as it determines whether or not the applicant will be offered credit (credit history and verification of customer's documents) and how much (credit score). Various levels of banking staffs, officers (Loan Sourcing Officer, Loan Processing Officer, Loan Sanction Officer, Control Officer etc.) , outsource agents (Advocate, Valuers etc.) and outside agents are intricately involved in this credit appraisal phase.

Once these first two phases are over successfully, credit sanction process commences. This phase is a completely internal banking process and involves Loan Sanction Officer and Control Officer. These two officers decide how much credit is to be sanctioned .The customer is not involved at this stage.

Final credit disbursement involves customer who has to be summoned by the bank to complete the formalities to receive the credit (either in full or instalment).

The next stage is the credit repayment (normally by instalment) by the customer. If the repayment by the customer becomes irregular, then the next stage i.e. credit monitoring becomes important.

Credit monitoring involves (a) monitoring irregularity in customers' repayment pattern (b) segregating customer portfolio according to duration of repayment irregularity. If the repayment pattern becomes highly irregular (non-repayment for three months or more) then that particular portfolio is termed as NPA (Non-Performing Asset).

With the automation, the management is able to track list of defaulter at the branch level, Loan Processing Cell and Account Tracing Department. Normally the management will go for soft recovery measures like phone call, SMS, face to face meeting etc. to persuade the defaulter to pay up. If soft persuasion technique is not successful, the bank may identify those portfolios where this technique failed. In this case the bank may go for detailed scrutiny and further segregate the defaulter NPA portfolios into the following two categories (a) non-wilful defaulters (b) wilful defaulters.

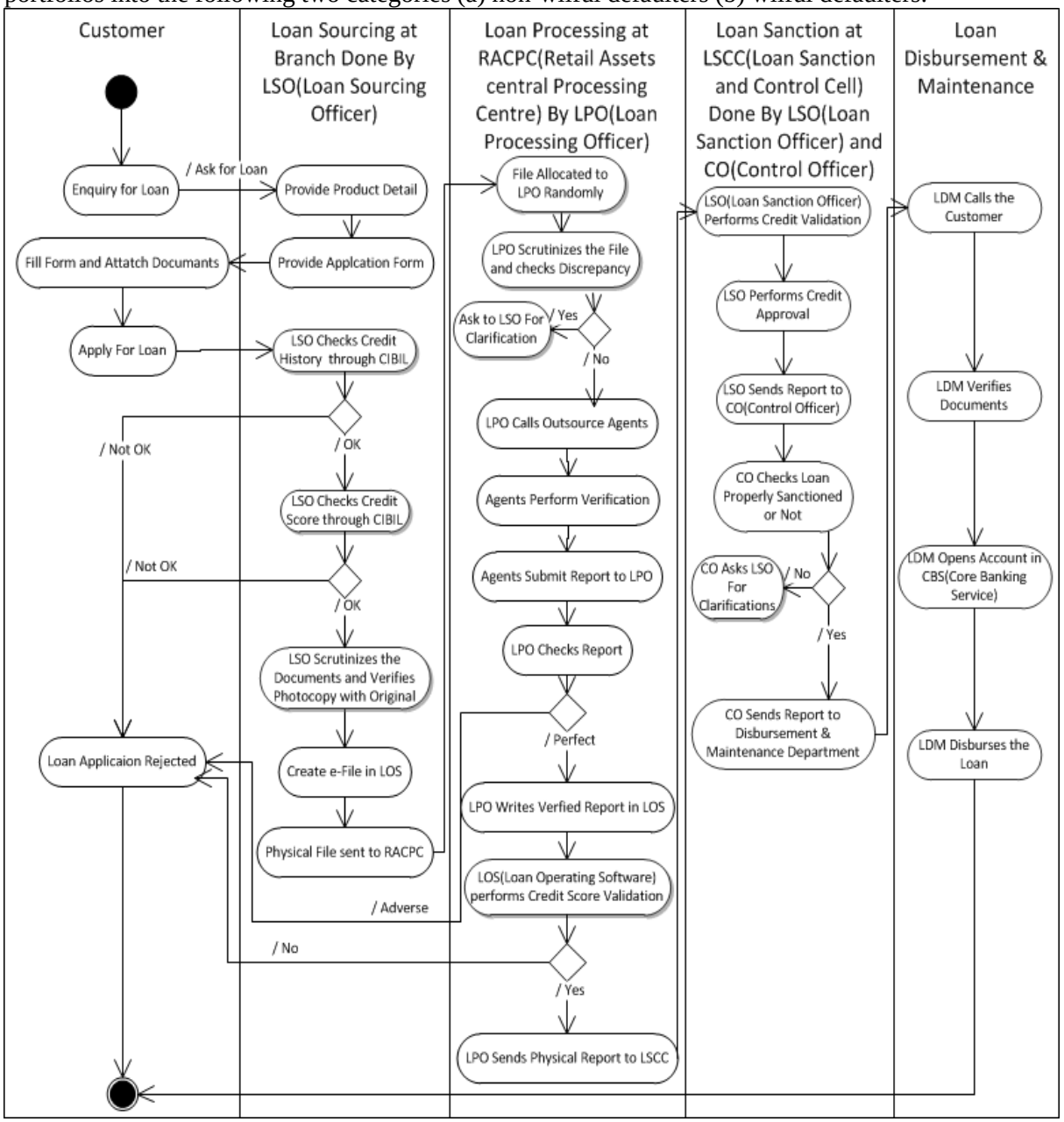

Figure 3. Credit Management Process for Small and Medium Sector in the Bank

For non-wilful defaulters the bank management is concerned about the genuine hardship (bankruptcy, difficult business scenarios, natural calamities etc.) faced by the defaulters. In such scenarios management often renegotiates with the defaulting customer about terms of loan repayment, payment duration as well as interest rate. Customers sometimes demand of partial waiver of loan or opt for staggered loan repayment.

For wilful defaulters bank often takes recourse to more stringent and formal approach. Sending legal notice, filing money suits in courts, publishing names and photographs of defaulters in media (print and electronics), invoking SARFESAI act to auction defaulters mortgaged properties to recover proceeds are some of the more formal approaches resorted to the bank management.
For more difficult cases, bank often takes help of the outside recovery agencies. Bank club together and sell some of the portfolios (called "stressed asset" whose recovery probability is extremely low) at fraction of their original values to the recovery agencies. The latter often employs quasi-judicial methods (coupled with strong arm tactics) to recover the proceeds from the recalcitrant defaulters.
The entire process of credit management is shown in the Figure 3.

8.2 Activities of Banking Agents in Credit Management in SME (Small and Medium Enterprise) Sector in Bank

In the credit management operations in SME sector there are seven principal agents/actors viz. Customer, Bank Staff, Bank Management, Bank Outsource Agents, Outside Agent (representing outside world), Auditor and Bank Board of Directors. The last agent (Bank Board of Directors) is mainly concerned with the policy issues and do not take part in day to day activities. While doing the activities, the various agents willingly or unwillingly commit many deviations from the prescribed rules and regulations laid down in the banking norms. The agents commit the mistake/deviations due to various complex circumstances including agents' group behaviour, agents pay off matrix, various incidents, internal state of the agents including agents' mental state and so on. This has been illustrated in Figure 2 above. For the auditor the crucial thing is the deviation component illustrated in the Figure 2. As the deviation component is being calculated in an unstructured domain, the challenge is to measure it. The Table 4 illustrates major activities, sub-activities, compliance rules and its violations as well as the involvement of group of agents in the credit processing in SME sector in the bank.

Sl. no	Major Activities of the agents	Detailed Sub Activities of the agents	Compliance Rules	Violations of Compliance Rules	Groups of Agents Involvement
1.	Undertake diligent pre-sanction screening process for borrowers/ guarantors	Verification (name, age, gender, nationality, marital status , identity verification, address proof , income proof) of customer/guarantor	Scrutinizing and verifying authenticity / genuineness of submitted documents	Fraudulent documentation	Customer, bank staff, bank management, bank outsource agents, outside agent , auditor
2.	Undertake evaluation of borrower's credit scorecard	loan amount, valuation of the property ,loan to valuation of property ratio, down payment amount ,loan repayment duration, applicant information (name, age, number of dependents , qualification, occupation, duration of service , designation, date of retirement , annual income, net worth, revolving debt)	Adherence to standard controls	Lack of oversight by staff/management on deviations from	bank staff, bank management, bank outsource agents, auditor

				existing controls	
3.	Undertake borrower's credit history appraisal prior to loan sanctioning	Undertake privileged information retrieval and sharing of borrower's credit history	Adherence to standard operating procedure	Violation of standard operating procedure/guideline	bank staff, bank management, bank outsource agents, auditor
4a.	Scrutinize/Verify following submitted Information by the Applicant for Loan Processing	Personal Profile ((name, age, gender, nationality, marital status , identity proof , contact details , address proof , income details, professional /educational qualification, occupational details, net worth, movable and immovable properties), Bank Account(s) details, Financial Information, Existing Investments, Details of Existing Loans/ Instalment Payment, Details of Immovable Properties, Purpose of loan, Cost of property, Sources of fund, Proposed Repayment Mode (Cheque off facility, Salary Account with SI, PDC), Repayment Period	Verify authenticity / genuineness of submitted documents	Fraudulent Documentation	Customer, bank staff, bank management, bank outsource agents, outside agent , auditor
4b.	Scrutinize submitted Documents (duly attested) by the Applicant for Loan Processing	Sale Deed /Agreement of Sale, Copy of approved drawings of proposed construction/purchase/extension, NOC from competent authorities, Detailed cost Estimate / Valuation Report from Chartered Engineer/Architect, In case of conversion of agricultural land for non-agricultural purposes, copy of the relative order, Non Encumbrance Certificate for 13 years, Salary Certificate, IT Returns for the last 2 years, Allotment letter of Co-operative Society / Housing Board (if applicable), in original, NOC from society/builder, Proof of residence (Identity Card/Passport/Voter Identification Card/Driving licence), Tax paid receipts etc. (Advance IT/Property Tax/Municipal Tax, etc.), other documents if any	Verify authenticity / genuineness of submitted documents	Fraudulent Documentation	Customer, bank staff, bank management, bank outsource agents, outside agent , auditor
5.	Due Diligence for verification of scope and credentials of outside agents prior to empanelment	Past experience and competence , Financial soundness and ability to service commitments, Business reputation and culture, compliance, complaints and outstanding or potential litigations , Security and internal control, audit coverage reporting and monitoring environment, business continuity management , Due diligence for sub-	Defining and executing outsource criteria, performing due diligence prior to selection , reporting significant fraud/violation to the controlling authority, Access to books and	External Vendor induced fraud	bank management, bank outsource agents, auditor

		service providers ,Risk management, Secure infrastructure facilities ,Employee training, knowledge transfer ,Reliance on and ability to deal with sub-contractors	records and inspections, Selecting performance metric, Scrutinize performance monitoring, , access to information on need to know basis, awareness of security and privacy policy,		
6.	Review Service Level Agreement (SLA) and Performance Metric	Formal SLA policy ,SLA monitoring process , Recourse in case of non-performance , Escalation metrics , Dispute resolution process , Conditions for mutual/one-sided termination	Scrutinize Service Level Agreements, identify obligations and liability in the event of a service contract breach	External Vendor induced fraud	bank management, bank outsource agents, auditor
7.	Incorporating Termination Clause while engaging with the outsource agents	Inclusion of termination clause and minimum periods for execution, confidentiality and non-disclosure agreement, conditions for default termination / early exit option for contracts , an appropriate handover process for data and process	Scrutinize Termination Clause, identify obligations and liability in the event of invoking of termination clause	External Vendor induced fraud	bank management, bank outsource agents, auditor
8.	Undertake verification of actual physical existence of collateral	Verification of actual physical existence of the Properties /Collateral	Selection amongst empanelled lawyers, Searching out from relevant Selection amongst empanelled valuers, Searching from Govt. Department/Registry Office	Non-existence of Collateral	Customer, bank staff, bank management, bank outsource agents, outside agent, auditor
9.	Undertake more than one counter verification if loan portfolio is beyond a certain value	Verification of actual physical existence of the Properties /Collateral	Selection amongst empanelled valuers, Selection amongst empanelled lawyers, Finding out relevant rate of properties in the concerned areas, Cross-checking with previous valuation	Non-performing SOP (Standard Operating Procedure)	Customer, bank staff, bank management, bank outsource agents, outside agent, auditor
10.	Verification/counter checking if mortgaged properties are transferred illegally	verification and ownership matching of actual physical existence of the Properties /Collateral to the borrower	Selection amongst empanelled lawyers, Selection amongst empanelled valuers, Searching out from relevant sections in Govt. Department /Registry Office	Transfer of Mortgaged Collateral without Sanction/ Knowledge /Permission from the Bank	Customer, bank staff, bank management, bank outsource agents, outside agent, auditor
11.	Undertake valuation for customer's (borrower's)	Verification of the Properties /Collateral being under/overvalued for mortgage,	Selection amongst empanelled valuers, Selection amongst empanelled lawyers,	Overvaluation/Undervaluation of Propertie	Customer, bank staff, bank management, bank outsource

	mortgaged properties or collateral		Finding out relevant rate of properties in the concerned areas	s/Collateral	agents, outside agent, auditor
12.	Verification if the identical mortgage is not reused to obtain multiple loans from multiple sources	verification and ownership matching of actual physical existence of the Properties /Collateral to the borrower and previous mortgage history of the property/collateral to the bank/lending agency	Selection amongst empanelled lawyers, Selection amongst empanelled valuers, Searching out from relevant sections in Govt. Department /Registry Office	Obtaining Multiple Loan on same properties	Customer, bank staff, bank management, bank outsource agents, outside agent, auditor
13.	Verify if the identical mortgage is resold without Sanction /Knowledge /Permission from the Bank	verification and ownership matching of actual physical existence of the Properties /Collateral to the borrower	Selection amongst empanelled lawyers, Selection amongst empanelled valuers, Searching out from relevant sections in Govt. Department /Registry Office	Sale of Mortgaged Collateral without Sanction/ Knowledge /Permission from the Bank	Customer, bank staff, bank management, bank outsource agents, outside agent, auditor
14.	Verify if loan sanctioning process /amount is within sanctioning authorities' jurisdiction/permissible limit	Verification of codified power of sanctioning authority		Incorrect Sanctioning	
15.	Verify if any agent exceeded its sanctioning power	Verification of codified power of sanctioning authority		Misuse of Power of Attorney	
16.	Verify if proper due diligence (including physical verification of site, mortgaged asset etc.) has been performed prior to loan sanctioning				Customer , bank staff, bank management, bank outsource agent, bank outside agent, auditor
17.	Undertake penal Provision against	Review SLA (Service Level Agreement)and Performance Metric (Activity 6),	SLA , Performance Metric, Terminal Clause	Violation of standard operating	Bank management, bank outsource

	Bank's Empanelled Advocate /Valuer / Consultant for professional improprieties or dereliction of duties	invoke Terminal Clause, if warranted (Activity 7), invoke penal provision if required		procedure/guideline	agents, outside agent, auditor
18.	Provision of close monitoring of loan accounts with irregular reimbursement and recovery	Daily Branch Level Report (Failed Standing Instruction Report) , Irregularities Report (Monthly), Sending defaulter SMS , phone call, meetings … , Loan Processing Cell, (Maintenance Unit), Soft Recovery Measure, , Account Tracing Department, Telephonic Call , Hard Core NPA Recovery Cell	Banking rules and regulations for loan recovery and provision, loan restructuring, loan repayment duration, staggered payment, deferred payment, restructuring interest rate etc.	Violation of standard operating procedure/guideline	Customer, bank staff, bank management
19.	Strategize dealings with NPA (Non-Performing Asset)	Find out degree (soft, medium, hard core) of NPA through interaction with customer, Take appropriate measure (Activity 18 and 20) as deemed fit.	Banking rules and regulations for loan recovery and provision as well as legal actions	Violation of standard operating procedure/guideline	Bank management, bank outsource agents, outside agent, auditor
20.	Strategize for hard core NPA (Stressed Asset Management Branch)	Sending Legal Notice, filing money suit in courts, Serving notice under SARFESAI ACT. Publishing names of defaulters, Publishing photographs of defaulters, Auctioning the property, Handing over more difficult cases to outside recovery agencies	Banking rules and regulations for loan recovery and provision as well as legal and penal actions	Violation of standard operating procedure/guideline	Bank management, bank outsource agents, outside agent, auditor

Table 4. Activities of Agents in Loan Management in SME Sector of a Bank:

8.3 Deviant Activities of Banking Agents in Credit Management in SME (Small and Medium Enterprise) Sector in Bank

These are the two basic types of violations in credit management in banking industry, viz. Policy Based Violations ((a) Misuse of Power of Attorney (b) SOP Violations (Improper Sanctioning of Credit) (c) Diversion of Credit) and Entity Based Violations ((a)Over-valuation of Collateral / Non Existence of Collateral (b) Fraudulent Documentation (c) Fraudulent Instrumentation (d) Identity Theft and Mismatch (e) Account Takeover (f) Theft (g) Cyber Fraud (h) Multi Party Collusion. These broad patterns were detected from the portfolio of cases we have collected so far. There are areas in which both the areas (policy based and entity based) overlap. While Table 5 illustrates the Policy Based Violations , Table 6 illustrates Entity Based Violations in detail.

Sl. no	Misuse of Power of Attorney	Violation of SOP (Standard Operating Procedure)	Diversion of Loan
1.	Loan sanction without undertaking diligent pre-sanction screening process for borrowers/ guarantors	Loan sanctioned without proper documents (sanction letter, mortgage documents,	Borrower misused/ diverted the credit in

		due diligence, mortgaged property already sold out, Title dead found fake, Deed is in the name of another person, guarantor lived abroad)	other purpose
2.	Credit limit enhancement on fake mortgaged property	Wrong /illegal Sanctioning of loan (without pre-credit visit, enquiry, end user verification.)	Siphoning of Money to other account other than for which it was originally sanctioned
3.	Fraudulent increase of Overdraft amount	Loan sanction without repayment capacity	
4.	BM sanctioned various loans to fake enterprises	Loan amount, instalments limit, total repayment period etc. are beyond the prescribed limits	
5.	Issue of Duplicate Cheque Book/ Pass Book without Authorization	Loan sanctioned without address verification, KYC norms, signature authentication etc.	
6.	Transfer money illegally from customer A/c to dead/fictitious customer A/c/ personal/relative A/c and withdraw		
7.	Transfer amount to Intermediary General Ledger(IGL) A/c /Suspense A/c and withdraw		

Table 5. Policy based Violations of Agents in Loan Management in SME Sector of a Bank:

Sl. No.	Over valuation /Non Existence of Collateral	Fraudulent Documentations	Fraudulent Instrumentation	Identity Theft/Impersonation of Identity	Account Takeover	Theft	Cyber Fraud	Multi Party Collusion
1.	Non-existence of collateral	Fake Title Deed	Forged cheque	Modification /Alteration on Cheques	Subsidy disbursed in two parts on same date and amount drawn in	Stealing a monetary instrument/ cheque and	User Id and Password was hacked by Phishing attack	Connivance between customer and other parties (outside agents) to create fraudulent documents

					SB account and account closed after withdrawal	then opening an A/c to misappropriate the cheque		
2.	Non-existence of ownership (Fictitious /Dead Owner) of collateral	Fake sale deed	Double Payment on Cheque	Fake Signature	Modifying Book of Accounts to conceal forgery	Misuse and alteration of monetary instrument	Impersonating confidential user id and password	Customer colluding with panel advocates (outsource agents) in creating fake title deeds
3.	Partial-existence of ownership (Multiple ownership on collateral) of customer	Fake Land ownership documents	Fake Demand Draft	False Request to Alter Specimen Signature	Transfer money from customer A/c to dead customer A/c and withdraw balance		Siphoning off cash from ATM through hacking of confidential information/stealing ATM Card/ deactivating PIN	Collusion between bank officials and customers to sanction unauthorized loan
4.	Collateral already Mortgaged	Fake change registration documents	Fake Invoice	Non-existence/ fake existence of Beneficiary Account(s)	Opening account to expropriate fund meant for various government schemes		ATM card wrongly associated with other party account,	Bank Manager sanctioned various loan by deviating guidelines with the help of borrower, panel advocates, valuer and middlemen

							through wrong entry of account number to the ATM Card	
5.	Collateral sold out before mortgage	Fake stamp duty	Xerox copy or scanned copy of original cheques	Availing Loan using Fake Employee Certification	Loan sanction to fictitious people under PMRY, SJSRY,PMEGP		Illegal unauthorized transaction using user ID and password of other employee.	borrower with the help of vendor & middle men present fake documents of quotations and land ownership
6.	Litigated Ownership of collateral by customer	Genuine Title Deed of dead owner		Opening fake account to transfer fund from various customer account	Stealing a cheque and then opening an A/c to misappropriate the cheque			
7.		Revenue receipt is forged		Wrong handling over of cheque book to imposter claiming to be customer	An inoperative A/c convert into operative with deposit of Rs. 100, Submission without			

					signature slip. Rs.60000 Withdraw through fake signature.			
8.		Fake Stamp paper		Unauthorized Issue of Duplicate Pass Book to imposter claiming to be customer				
9.		Invalid AOS (Agreement of Sale)		Unauthorized Issue of ATM Card to imposter claiming to be customer				
10.		Fake Land Records		Loan availed by fictitious borrower /firm				
11.		Fake KYC		Submitting spurious KYC (Know Your Customer)				
12.		Forged TD		borrower and dealer are same person				
13.		Fake RC book,		Person changed his name slightly to avoid being detected after				

				availing multiple loans which were non-paid				
14.		Fake insurance paper						
15.		Fake physical inspection report of vehicle purchased						
16.		Fake salary slip						
17.		Fake Govt. Chelan						
18.		Fabricated financial statement						
19.		Fictitious purchase orders						
20.		Fictitious export bill						

Table 6. Entity based Violations of Agents in Loan Management in SME Sector of a Bank:

8.4 Measuring Deviation in Credit Management in SME (Small and Medium Enterprise) Sector in Bank

Auditing Various scores in auditing scorecard measures the deviations related to number of deviant sub-event a particular event is capable of generating. A deviant event may be classified by using two completely different strategies viz. by using (i) similarity functions (ii) impact functions. These functions are described below.

Similarity functions measures how the two patterns of events, which may be correlated, are similar to each other. It uses ontology mapping technique by which two sets of events are quantitatively measured to evaluate how (dis)similar they are. Once this measurement is known, the dissimilar events are penalized proportional to the deviant weights. The underlying assumption is that the events will generate deviant or fraudulent patterns proportional to the dissimilarity measurement. This method is akin to spot fine technique in which penalty imposed on the errant action is proportional to the future damage (with

some finite probability) it will cause. This model is very efficient in detecting dissimilarity but the drawback of the model is that the imposed penalty may not accurately predict future event or loss (due to probabilistic occurrence).
The other type of algorithm which measures deviation is based on actual impact function. It measures the actual loss accurately and then tries to find out the source of occurrence of event which caused the loss, but that may not be very efficient in detection. Hence the two methods may be classified according to efficiency/automation vs. predictability/accuracy.
Now let us see how our methods can be applicable for Over-Valuation/Non Existence of Collateral (Mortgage) which is a major source of violation in credit management.
The steps illustrated here for verifying existence of immovable properties has been depicted in Figure 3 in Section 8.1. The steps are stated as follows

(i) LSO at RACPC calls the two outsource agent (Panel Advocate, Property Valuer) to investigate and give report
(ii) Panel Advocate checks corresponding ownership between applicant and collateral with the help of outside agent and reports its findings to the LSO at RACPC. Failure therein will result in Non-Existence of Collateral being undetected.
(iii) Property valuer evaluates the correct price of collateral with the help of outside agent and reports its findings to the LSO at RACPC. Failure therein will result in Non Evaluation of Collateral being undetected.
(iv) LSO at RACPC evaluates the reports and takes suitable action.

Combinatorial (non-existence of collateral) of the investigation and reports may be stated as follows :

(i) Outside agent has eight findings for Property (P) and Ownership (O) between applicant and property $[P/\bar{P}] \times [ON/OP/OE/OD/OL]$. $[P/\bar{P}]$ represents two states viz. Property exists (P)/ Property does not exist ($\bar{P}$). [ON/OP/OE/OD/OL] represents five states viz. ON (Ownership Non Existent: owner dead, property sold out)/ OP (Ownership Partially Existent: multiple ownership of properties)/ OE (Ownership Exclusively Existent) OD (Deferred Ownership: property mortgaged)/OL (Ownership Litigated which corresponds to disputed property).Together they correspond to $2\times5=10$ states. Out of these 10 cases only one case corresponds to genuine case where property exist (P) and there is exclusive right of the applicant on the property OE (P&OE).
Outside agent sends (true/false) either of the ten reports to Panel Advocate who in turn sends (true/false) it to LSO. So there are $10\times2\times2=40$ combinatorial possibilities for this case alone. Out of them only one combination (P&OE&T&T) represent genuine case and its report.

(ii) Outside agent has three findings for Property (P) and its Valuations (V) (POV, PUV, PEV) [POV/ PUV/PEV] represents three states viz. Property Over Valued/Property Under Valued and Property Exactly Valued respectively. Outside agent sends either of the reports (POV, PUV, PEV) to Panel Valuer who in turn sends it to LSO. So there are $3\times2\times2=12$ combinatorial possibilities for this case alone.

The consequent events generated for verification of customer's ownership of immovable property are as follows

(i) In case of failure in (i) [Non Existence of Collateral simultaneity with failure on the part of Panel Advocate to detect it] will result in loss for bank to mortgage/sell off collateral in case of non-payment by defaulter. This will ultimately result in civil/criminal suit.
(ii) In case of failure in (ii) [Over valuation of Collateral simultaneity with failure on the part of Panel Valuer to properly evaluate it] will result in loss for bank to mortgage/sell off collateral in case of non-payment by defaulter. This will ultimately result in civil/criminal suit.

The events generated due to deviant actions of the various agents play a major role in determining risk impact and risk score illustrated in Table 3 in section 7.2 and which in turn influences variable

components in Table 2. Higher the number of possible deviant events more likely the chance of value of risk score being of higher magnitude.

9 LIMITATIONS AND FUTURE SCOPE OF WORK

As stated in the introduction the principal limitation lies in not defining construction of agent architecture (including algorithm and knowledge sharing among different ontologies) , due to space limitation of this paper. Similarly we could only show one component (out of possible ten components) of the audit score card viz. Revenue Leakage Component and its sub- components in somewhat greater detail but could not describe other equally important components and its effectiveness vis-a-vis audit score card as a DSS tool for the auditor(s) and banking system as a whole. Another limitation of the paper is that full evaluation of the benefits of our ontology based audit score card model will require many more comparative case studies from our portfolio of around 700 cases in banking domain under different situations , which again could not be taken up due to space constraints. One major challenge we would like to address in our future scope of research is how we could use the audit scorecard model to construct ontology which is sharable across two distinct domains (e.g. compliance auditing in banking and power sector). We would like to take up this critical challenge in our future scope of work.

10 CONCLUSION

Manual auditing process in Indian banking sector often failed to keep pace with rapid stride of digitization of core banking services. Co-existence of legacy systems as well as computerized core banking services often entangles banking processes and functionality with control requirements of GRC. In this paper we proposed a novel solution to manual auditing process by elucidating a model of ontology based automated audit risk score card. The design challenge of multi-layered architecture with different scope and granularity for knowledge representation in multiple ontology layers may be exploited for modular designing and reuse. That this model is suitable for automatically detecting anomalous and fraudulent patterns within banking transactional data has been elucidated succinctly. As knowledge based devices are normally efficient in prevention/detecting complicated anomalous patterns in a system, the audit score card as a prototype DSS tool may prove helpful for an auditor working in Indian banking sector.

References

Abdullah, S. N. H., Induslka , M. and Shazia, S,(2009) A study of compliance management in information systems research, in ECIS 2009 Proceedings. 2009.

Ashbaugh-Skaife , H. and Collins, D..(2008). The effect of SOX internal control deficiencies and their remediation on accrual quality. The Accounting Review, 83 (1): p. 217-250.

AusCERT,(2006) .Australian Computer Crime and Security Survey, http://www.auscert.org.au/render.html?it=2001&template=1, 2006.

Borst, W. N. (1997). Construction of Engineering Ontologies for Knowledge Sharing And Reuse. *Thesis*. The University of Twente, Netherlands.

Deloitte.(2012).Indian Banking Fraud Survey: Navigating the Challenging Environment.

Ernst & Young (2012) .Global Information Security Survey 2012.

FF POIROT, Semantics Technology and Applications Research Laboratory (STAR Lab), - http://www.ffpoirot.com/default.htm

Fisher, J.(2007). Compliance in the Performance Management Context: What technologies could simplify compliance and automate information gathering? Bank, Accounting & Finance, 2007. 20 (4): p. 41-49.

Gruninger, M. and Lee, J. (2002).Ontology Applications and Design. Communication of the ACM 2002/vol.45, No.2.

Hagerty, J. and Kraus, B. (2009), GRC in 2010 : $29.8B in Spending Sparked by Risk, Visibility, and Efficiency. 2009: Boston, MA. p. 12.

Heiser, J.(2010).Hype Cycle for Governance, Risk and Compliance Technologies, 2010, in Gartner Hype Cycles. 2010, Gartner Research Report G00205229.

Jamieson, R.(2003).Issues in e-Business Risk & Security Management, IEEE Fincom03, Sydney,July03.

Leary,R., Vandenberghe, W. and Zeleznikow, J.(2003). Towards a Financial Fraud Ontology; A Legal Modelling Approach", ICAIL Workshop on Legal Ontologies & WBLIM, June 2003, Edinburgh

Lau, G., Law, K. H,. Wiederhold, G.(2005). Legal Information Retrieval and Application to E-Rulemaking, In Proceedings of the 10th International Conference on Artificial Intelligence and Law (ICAIL), pp. 146-154, 2005.

Managesoft (2007).Managesoft Compliance Manager, http://www.managesoft.com/product/compliance/index.xml, Last Accessed: March 2007.

OpenPages(2009). Risk Management Investments to Rise in 2010. 2009.

Parry, E.,. (2004). SOX Wars: CIOs share ideas, fears on Sarbanes-Oxley compliance.SearchCIO.com.

PricewaterhouseCoopers.(2006)Information Security Breaches Survey. http://www.pwc.com/uk/eng/ins-sol/publ/pwc dtifullsurveyresults06.pdf

Saha,P. ,Pramesswaran, N. , Ray ,P and Mahanti,A(2011). Ontology Based Modeling for Information Security Management. presented at Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2011.

Symantec. (2006) .Improving IT Compliance: Guidance for Midsize Organizations, Whitepaper, July, 2006.

Teubner, R.A. and Feller, T. (2008) Informationstechnologie, Governance und Compliance. WIRTSCHAFTSINFORMATIK, 2008. 50 (5): p. 400-407

Volonino, L.,. Gessner, G.H, and Kermis, G.F.(2004). Holistic Compliance with Sarbanes-Oxley. Communications of the Association for Information Systems. 14.

Wiesche, M., Schermann, M. and Krcmar, H.(2011) Exploring the contribution of information technology to Governance, Risk, and Compliance (GRC) initiatives, Paper to be presented at the 19th European Conference on Information Systems (ECIS). 2011: Helsinki, Finland

Wong, A. K. Y., Yip,F , Ray, P., Paramesh, N.(2006). "Semantic Data Integration for IT Governance", presented at International Workshop on Semantic e-Science, Co-located with ASWC06, Sept 2006.

Wong, A. K. Y., Yip,F , Ray, P., Paramesh, N.(2008). "Towards Semantic Interoperability for IT Governance", accepted in Computing and Informatics Journal , January 2008