# Development of Ontology Based Framework for Information Security Standards

Partha Saha
MIS Group
IIM Calcutta
Kolkata, India
shree.partha.saha@gmail.com

Ambuj Mahanti
MIS Group
IIM Calcutta
Kolkata, India
am@iimcal.ac.in

B.B. Chakraborty
Finance and Control Group
IIM Calcutta
Kolkata, India
bbc@iimcal.ac.in

Avinash Navlani
MIS Group
IIM Calcutta
Kolkata, India
avinashnvln8@gmail.com

***Abstract*— E-Business Management and associated risk mitigation of organizational resources have become a major challenge for the organizations in light of increasingly global and integrated digital economies. Our research focuses on information security in e-Business management. We consider, in particular, the domain of banking. The banking sector, being highly regulated, poses plethora of challenges in terms of compliance of organizational practices with regulatory standards such as Basel III, CobiT 4.1 and ISO17799. An automated compliance auditing solution to the existing manual auditing is highly desirable from management's standpoint due to considerable savings in cost and time. In this paper, we envisage a new paradigm where ontology based information model is used in an automated compliance auditing application. It performs compliance checking to verify if actual banking practices are following information security standards and whether discrepancies between security standards and actual banking practices call for qualified, adverse, disclaimer or piecemeal opinion by the information security auditor, while investigating efficacy of information security standards employed in banking domain**.

***Keywords-Information Security; Compliance Auditing; Risk Management; Indian Banking Regulation .***

## I. INTRODUCTION

Compliance Management (CM) is a business process that concerns organizations of different magnitude and size. It deals with the process of checking the organization practices with the regulatory compliance policies and business guidelines in an integrated and networked environment. This process is a continuous and labour intensive task that involves business and management's commitments, time and resources in demonstrating organizational alignment, adherence and compliance to the prevailing regulations and best practices (such as Sarbanes Oxley [9] , HIPPA [12], Basel III [21], CobiT4.1 [20] ). The importance of compliance is underscored from renowned corporate frauds like Enron and WorldCom [23]. In this paper, we are analyzing the application of ontology to (semi) automate compliance auditing process (a process which is till now completely manual). We try to address the fundamental research question of how we may segregate the compliance rules and regulations of a standard (CobiT4.1) and organization practice (that of a bank X in India, which is implementing CobiT4.1) into two different ontology layers (source and target ontology, respectively) which may facilitate automated compliance auditing. By comparing two ontologies, performance evaluation of the organization vis-à-vis source regulations may be ascertained. Although here we are applying our methodologies upon specific case of application of CobiT4.1 in banking domain, the application of the methodology is independent of any specific domain or standard.

The paper is organized as follows. Section II briefly discusses GRC (Corporate Governance, Risk Management and Compliance Auditing) while Section III undertakes literature survey. Section IV briefly expounds methodological framework of ontology based compliance auditing, while Section V discusses the compliance measurement in information security standards. Section VI applies the framework for an Indian bank X, while Section VII calculates the compliance metric for the bank X and discusses various scenarios. The paper concludes with Section VIII.

## II. CORPORATE GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE AUDITING (grc)

In this section, we will be briefly discussing about corporate governance, risk management and compliance auditing related to banking sector.

### *A. IT Governance and Regulatory Standards*

IT governance is a part of overall corporate governance process of any organization. Aligning Information Technology with the strategic goals of the organization, delivering promised value to the stakeholders, optimum utilization of critical IT resources, undertaking risk management and strict performance monitoring are some of the cornerstone of IT governance. In this subsection, we present two well-known regulations and standards.

#### *1) BASEL III*

Basel III, a brainchild of BCBS (Basel Committee of Banking Supervision) [21], (which came into effect starting January 1st, 2013) is equipped with twin legal instruments namely: Directives and Regulations. The Directive contains four cardinal principals, namely: (i) Increased Governance (ii) Capital Buffer (iii) Increased Supervision and (iv) Sanctions. The Regulation part contains five important sections, namely: (i) Definition of Capital (ii) Credit Risk from Counterparty (iii) Risk of Liquidity (iv) Single Rule Book and (v) Leverage Ratio [21]. With these set of stipulations, BCBS is trying to strengthen corporate governance, enhance banks' risk management capability, transparency and disclosure [21].

*2) Control Objectives for Information and related Technology (CobiT )*

CobiT has been developed by the IT Governance Institute and it provides reference framework for good IT standards and practices. It is a tool that is used by the Information Security auditors and practitioners alike. CobiT includes a framework that responds to the management's need for adequate control and measurement of IT by providing tools to standardize, assess and measure the organization's IT resource and capabilities vis-à-vis thirty-four CobiT IT processes [20].

### *B. Risk Management in Indian Banking Sector*

Over the last couple of decades, India has emerged as one of the fastest growing economies in the world (average 7% GDP growth). India's banking and financial institutions have also experienced high growth rate (18% growth in banking sector) [14]. Rapid stride in ICT (Information and Communication Technology) has helped Indian banking industry to metamorphose from a ledger driven manual activity to a pervasive, fully networked and integrated CBS (Core Banking Services) system. But the undeniable consumer benefits are often offset by techno-procedural complexities in risk management in B2C (Business-to-Consumer) environment. It gives rise to multifarious frauds of alarming proportions [14]. Hence appropriate controls (policies, procedures, guidelines, processes etc. across organizations) need to be implemented to contain the menace.

### *C. Compliance Auditing (CA)*

As evident from a recent Ernst & Young Global Information Security Survey-2012 [18], stakeholders are increasingly concerned over frauds endangering confidentiality, integrity and security of the organization's information repository. Consequently, organizations are encumbered with the task of synchronizing day to day activities and procedures with a host of standards, regulations and guidelines which are legally binding. CA or Compliance Auditing (which is part and parcel of any regulatory compliance process), formally states whether mandatory controls and safeguards are employed and function correctly. But, without automation, it becomes difficult to manually correlate business practices with conflicting statutory requirements and industry best practices.

## III. LITERATURE SURVEY

In the banking sector, information asymmetry among cooperative/competing agents is one of the root causes of fraud. Anonymity of agents' actions (in different physical and digital channels and payment avenues) results in a state of non-equilibrium of trust and controlling power among interacting agents. Some of these agents try to exploit lacunae in the banking process and technology. This chain of events gives rise to the scope for fraud [16]. Deloitte's fraud survey on Indian Banking sector brings some of these disturbing trends into the open [14]. According to the survey respondents, "lack of oversight by line managers and/or deviations from existing process/controls" (73%), "current business pressure to meet target" (50%), "difficult business scenarios" (47%), and "lack of automated tools to identify potential red flags" (37%), "collusion between internal staffs and external agencies" (37%) are five major reasons for fraud [14]. All these point to the cardinal importance of automated Compliance Auditing (CA) solutions for information security and mitigation of fraud.

Vendor/technology specific computer-assisted compliance management solutions exist which address a small subset of problems within compliance and primarily focus on lower-level aspects of IT governance such as configuration management, change management, patch management and licensing management [8] [10].

In this paper, we utilized many concepts from diverse fields e.g. fuzzy reasoning system [6] [7] [13] and ontology, which are adopted from ontology engineering [1] [2] and ontology learning [3]. These techniques, along with linguistic tools [4], are used to (semi) automatically extract a body of concepts, relationships and values from various information sources (e.g. employee handbook) to form an ontology. Fuzzy reasoning has also been applied in other important domains such as law, healthcare and financial engineering [5] [11] [13].

## IV. METHODOLOGY

Current research involving creation of ontology based adaptive automated CA system belongs to the design science [19]. Ontology, which is frequently referenced, is "an explicit specification of a shared conceptualization of a domain" [2] [11]. It is constructed to capture implicit, explicit and commonsense-knowledge of a domain such that the knowledge may be shared, accessed, reused and consumed by autonomous computing agents. In this section, we will show how ontology may be used to capture compliance auditing process into reference and target knowledgebase which facilitates organization's performance measurement during auditing.

### *A. Ontology of Information Security Concepts*

The study will identify a set of notions, viewed as important, in the context of information security. The notions are then defined as concepts. For each concept, the intuitive meaning is documented and the relationships between the concepts are simultaneously derived. The concepts and the relationships are then used to design the ontology. At the same time, any additional attributes, required by the ontological concepts, are categorized. In the next two sub-sections, we divide the conceptual framework in reference and target ontologies.

### *B. Reference Ontology*

Our application, namely construction of reference ontology, is divided into the following three steps: (i)

Domain Knowledge Modelling (ii) Application Logic Modelling (iii) Application Logic Extension.

(i) Domain Knowledge Modeling: it can be formalized from the following knowledge sources: Information Security Standards and Best Practices (e.g. ISO17799 [17], CobiT4.1 [20]), Information Security Dictionaries (e.g. Glossary for Information Security), Domain Experts Knowledge etc.

(ii) Application Logic Modelling: it can be extracted from the following important knowledge sources: Compliance Requirements from Information Security Standards, Contractual Agreements with Stakeholders, Company Policies (e.g. Employee Handbook) etc.

(iii) Application Logic Extension: it can be formalized from the following knowledge sources: Past compliance results, Business Impact Assessment (BIA), Analysis of financial penalty due to non-compliance etc. Section V will elucidate the entire approach while modelling PO9 of CobiT4.1 [20].

### C. Target Ontology

Target knowledge base is the *Corporate Memory* of the organization. It contains the facts and knowledge about the organization. The knowledge can come from the following sources: Document Management Systems (e.g. knowledge and Meta data), File systems (e.g. instances of documents stored in network drives), Employee Management System (e.g., knowledge of organization entities) etc.

### D. Compliance Rules and Metrics

In order to perform a compliance study, the agent behaviours are to be captured and verified in a particular scenario. Next, it is to be ascertained whether the behavioural trace is consistent with the regulatory requirements. Compliance measure is computed by first converting the compliance rules, expressed in EC (Event Calculus), into a set of high level language like Java. Each node in the tree represents an event (primitive or abstract) spread over an interval of time. Using temporal relations, an event node is related to one or more nodes, at the primitive level.

### E. A Fuzzy Technique for Adaptive Compliance Auditing

In the ideal world, all compliance knowledge and facts are properly captured and stored in an ontology. Thus, machines can confidently reason and infer results based on the precise and complete data. However, this is not the case in the real world, where most of the data is imprecise, incomplete and ambiguous in nature. To capture the imprecision and uncertainty of the real-world knowledge, we make use of Weighted Fuzzy Production Rules (WFPRs), as a mechanism to represent our compliance requirements.We try to mimic the real world scenario of an auditor( who is adjusting and tolerating numerous imprecise or missing compliance data), while (s)he is in the process of concluding whether compliance is achieved or not for the organization. We propose the use of fuzzy logic techniques to address the inherit issues of vagueness and imprecise inferencing in automatic Compliance Auditing[1] [7] [13].

## V. COMPLIANCE MEASUREMENT OF INFORMATION SECURITY STANDARDS

In this section, we closely follow the methodology which was envisaged while constructing reference ontology in Section IV B. Here, we try to model a specific part of a principal security standard viz. CobiT4.1. Implementation of CobiT 4.1 has become mandatory in designing information security in most of the banks in India.

Information, along with systems, networks, hardware, software and supporting processes, are considered valuable assets to any organization. Protection of vulnerable information assets from wide range of threats, mitigation of business risks, ensuring business continuity, maximizing business opportunities etc. may be formally termed as information security. Complete modelling of a particular security standard like CobiT4.1 is beyond the scope of the present paper. Hence, we would like to show the methodology by rendering a part of the CobiT 4.1(Sec. PO9 of CobiT4.1 “Assess and Manage IT Risk”) into ontology based semantic modeling.

*a)* PO9 from CobiT4.1 establishes an IT risk management framework. It is followed by establishing particular context in which risk assessment framework is applied. Subsequently, specific risky events (events which are capable of producing negative impacts) are identified. Finally, risk response, maintenance and monitoring of risk action plan are undertaken.

*b)* Recommendations from PO9 from CobiT4.1. are expressed in the following steps:

- Deriving a semantic model (using ontologies from the view point of compliance checking) for information security standard. This model is derived from control statements and auditor’s queries.
- Deriving semantic rules from control statements.
- Applying the rules in the ontology database for checking consistency.
- Deriving strategies for handling partial, incomplete, erroneous and fraudulent data in the ontology.
- Determining the relevance of each concept (using fuzzy weights) for the computation of compliance.
- Computing the compliance measurement.

*c)* As robust risk management framework is an essential ingredient of Cobit4.1 security regime, the auditor may enquire from the company executives, whether following actvities have been properly performed no not.

i. Performing risk assessment.
ii. Evaluating strategic/tactical/ business objectives.
iii. Identifying internal/external critical IT objectives.
iv. Identifying risk context (Environment, domain, country, regulation, size, etc.).
v. Identifying events (business oriented, IT related).
vi. Assessing risk associated with each event (Record & maintain risk registry, cost, benefit etc).

vii. Identifying strategic risk associated with business (Investment, funding, technology, domain etc.).
viii. Identifying tactical risk associated with business (Project plans, implementation and other operational issues).
ix. Selecting, identifying, calculating risk responses.
x. Prioritising controls for risk mitigation.
xi. Providing appropriate funding policies in place for risk treatment.
xii. Maintaining a risk action plan.
xiii. Performing IT value management (Costs, benefits, Strategy and Tactics).

In Fig. 1, CobiT risk management framework is illustrated for our (partial) source ontology construction. Now, let us critically examine the methodology for the first question (whether or not the company on its part has undertaken proper risk assessment). In Fig. 1, CobiT 4.1 risk management framework is expressed in event based ontology representation. Each box in the Fig. 1 represents an event. The thirteen questions mentioned above may be enquired using structured query language. Here, the model is being represented using Event Calculus (EC). It is a logic formalism used for workflow analysis [22]. In a workflow process represented by EC, there are four major types of activities: (a) sequential activity (b) parallel activity (c) conditional activity and (d) iterative activity [22].

While examining risk assessment in Fig. 1, we work in a bottom-up manner. Setting up risk portfolio is preceded by two sub events (a) identify IT tactical risk and (b) identify IT strategic risk. This can be represented in Event Calculus by AND-join of concurrent activities. The formulation is shown below:

happens (end (set risk portfolio), T) ← happens (end ((identify IT tactical risk), T1), happens (end ((identify IT strategic risk), T2), T = max ( T1, T2) (1)

In a similar manner, risk categorization process can only start when the two sub-processes (setting up risk portfolio and identifying risk trends and events) are over. It is also represented in Event Calculus by AND-join of activities. The Event Calculus formalism is shown below:

happens (end (categorize risk), T) ← happens (end ((set risk portfolio), T1), happens (end ((identify risk trends and events), T2), T=max (T1, T2) (2)

Selecting risk commences sequentially after risk categorization is over and it is represented as:

happens (start (select risk), T) ← happens (end (categorize risk), T) (3)

Establishing risk context is composed of three sub processes (identifying external and internal context of each risk assessment, selecting risk criteria and selecting goals of risk assessment). These sub processes are also interlinked among themselves. Event Calculus formalism of AND-join activities is shown below:

happens (end (establish risk context), T) ← happens (end ((identify internal/external context of each risk assessment), T1), happens (end ((select risk criteria), T2), happens (end ((select goals of risk assessment), T3), T=max (T1, T2, T3) (4)

And, finally, risk assessment is complete after its sub-processes viz. selecting critical IT objectives, establish risk context and selecting risk are complete.

happens (end (assessing risk), T) ← happens (end ((select critical IT objectives), T1), happens (end ((establish risk context), T2), happens (end ((selecting risk), T3), T=max (T1, T2, T3) (5)

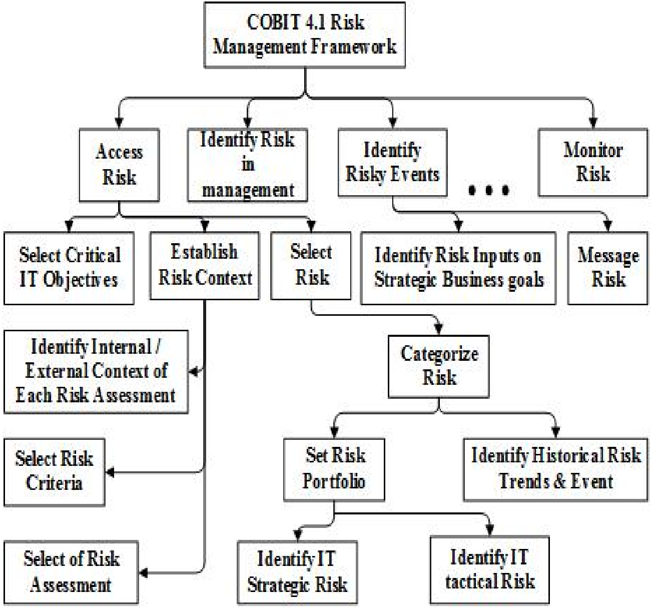
COBIT 4.1 Risk Management Framework
Access Risk
Identify Risk in management
Identify Risky Events
• • •
Monitor Risk
Select Critical IT Objectives
Establish Risk Context
Select Risk
Identify Risk Inputs on Strategic Business goals
Message Risk
Identify Internal / External Context of Each Risk Assessment
Categorize Risk
Select Risk Criteria
Set Risk Portfolio
Identify Historical Risk Trends & Event
Select of Risk Assessment
Identify IT Strategic Risk
Identify IT tactical Risk

Figure 1. CobiT risk management framework (partial source ontology)

Now, we discuss the same question, (i.e. risk assessment) in a top down manner, in finer detail. We closely examine each of the events in Fig. 1. We try to understand five processes: (i) temporal and causal relationship between events (ii) resource consumption by each event (iii) agents' relationship for each event (iv) the agents' organization associated with each event and (v) objectives of each event. The risk assessment event is composed of three sub events: (a) selecting critical IT objectives (b) establishing risk context and (c) selecting risk. The sub-goals coming in the form of attributes, value and relationship tuple are associated with each event (i) achieving business and IT alignment, priority matching and integration of purposes (ii) assessing business requirement in line with particular enterprise requirement, government regulations, relevant laws and contracts (iii) assessing capabilities and setting of performance metrics in terms of IT's contribution to organizations' goals, objectives, functionality, scalability etc. (iv) setting up of IT strategic and tactical plans (v) performing IT portfolio management by analyzing program portfolios, project and service portfolios (vi) performing IT value management by calculating project costs, benefits, strategy and tactics.

Next, we consider establishing risk context event which is subdivided into three sub-events, namely: identifying internal/external context of each risk assessment, selecting risk criteria and selecting goals of risk assessment. Internal and external risk context is dependent on specific environment like industry, domain, area, country, rules, regulations, best practices, financial health etc. Selecting risk criteria determines organization's risk tolerance. Selecting goals of risk assessment emphasizes that risk mitigation strategies are encoded within organization culture.

IT strategic risks are concerned with interaction of related stakeholders, strategic matching between IT goals and enterprise vision, investment opportunities, budget and funding, technology maturity etc. The tactical risks are concerned with IT-enabled program investments, IT initiatives in different projects, resource requirements etc. Finally identification of historical risk-trends and events are concerned with setting up of archives of historical cases (it records system failures, that seriously compromised performance).

## VI. RISK MANAGEMENT FRAMEWORK OF A BANK X

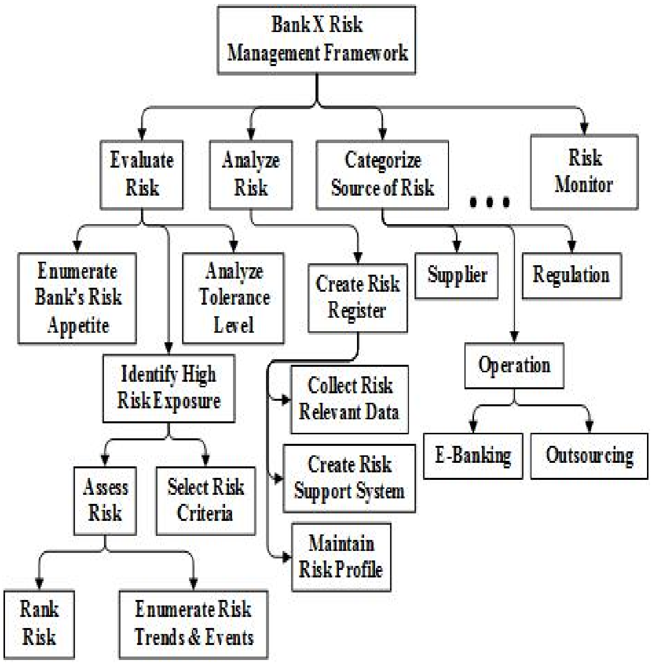
Bank X Risk Management Framework
Evaluate Risk
Analyze Risk
Categorize Source of Risk
• • •
Risk Monitor
Enumerate Bank's Risk Appetite
Analyze Tolerance Level
Create Risk Register
Supplier
Regulation
Identify High Risk Exposure
Collect Risk Relevant Data
Operation
Create Risk Support System
E-Banking
Outsourcing
Assess Risk
Select Risk Criteria
Maintain Risk Profile
Rank Risk
Enumerate Risk Trends & Events

Figure 2. Risk management framework of Bank X (partial target ontology )

In this section, construction of target ontology is envisaged as per guidelines in Section IV C. As per our case study, we are surveying a bank X in India. The bank X has over 1500 branches and offices and is having a total business turnover of more than $20 billion. Presently, bank X is having a three-tier organizational set-up (consisting of the head office, over 25 regional offices and the branches). Operations of all the branches have been computerized with ATMs and EFTS (Electronic Fund Transfer System). Risk management framework of the bank X closely follows risk governance framework of Cobit4.1.

The risk management process begins with risk appetite, risk tolerance level and risk exposure of the bank X. Identifying risk, analyzing, evaluating and ranking risk processes, controlling, monitoring and articulating risk impact on information and electronic assets will comprise risk governance of the bank. It is achieved by conducting the following exercises:

(a) Performing bank X's enterprise risk assessment.
(b) Evaluating IT risk tolerance threshold.
(c) Approving IT risk tolerance.
(d) Aligning IT risk policy with bank X's overall risk policy.
(e) Promoting IT risk consciousness/awareness culture among stakeholders.
(f) Useful communication of IT risk.
(g) Approving/accepting IT risk analysis.
(h) Enriching strategic decision making process using IT risk analysis.
(i) Prioritizing IT risk response activities.

Risk register or more popularly "risk log" is used for three specific purposes.

(a) Storing important data for accumulating, identifying, analysing, managing and reporting IT specific risk.
(b) As part of risk profile maintenance, an up to date inventory of known risk related events and the attributes (disposition, probable impact and expected frequency of occurrence) of IT resources are formed.
(c) Preparation of decision support system (with respect to risk management framework) is composed of defining / estimating IT risk and identifying risk response options.

Categorization of various sources of risk, is of paramount importance in bank X's risk governance framework.

(a) Board approved policy, procedure, guidelines.
(b) Digital signature and evidence (which is taken as legal proof) may be the source of fraud/malpractice.
(c) Suppliers/contractors are possible sources of risk.
(d) Adherence to stipulated privacy requirements of customer(s), where the bank is delivering various products/services through electronic banking channels (here the jurisdiction is domain and country specific).
(e) Granting authorization on need based requirements.
(f) Monitoring persons with elevated access privilege.
(g) Appropriate job profiling.
(h) Evaluating vendors/outsourced services providers (comprehensive due diligence procedures, monitoring performance, managing service-level agreements).
(i) Operational risk related to e-banking and outsourcing.
(j) Elimination/restriction on manual intervention for back up, update and data transfer.
(k) Proper authorization of data in foreign banks having access to bank X's data.
(l) Compliance with regulatory, statutory and contractual obligations on the deployment of Information Systems.

Depending on risk appetite of the bank and its impact/significance to the business, bank X management may take recourse to any of the following five actions:

(a) Ignoring risk (reject risk, if its impact is lower than the risk threshold).
(b) Avoiding risk (eliminate risk by removing causes).
(c) Transferring risk (deflect/ allocate/share risk with partners, insurance companies etc.).
(d) Accepting risk (formal acknowledgement of existence of risk and proper redress).
(e) Mitigating risk (reduce risk by defining, implementing and monitoring suitable procedures and safeguards).

While mitigating risk, management may choose to either use appropriate controls or reduce risk at acceptable level by using one or many of the following safeguards:

(a) Detailed inventory control of information and asset.
(b) Classification of new employees according to risk profile, priority and experience.
(c) Suitable physical and environmental control.
(d) Monitoring operational alignment with risk tolerance.
(e) Awareness training program for employees.
(f) Setting up robust incidence management process.
(g) Preparation of detailed audit trail.
(h) Providing data security measures like cryptography.
(i) Optimizing system security.
(j) Checking critical functions (finance, regulation, legal).
(k) Optimizing response to risk exposure.
(l) Implementing control for malware protection.
(m) Robust network protection strategy.
(n) Strong control for remote computing.

Communication of risk related issues to appropriate forum involves articulation and reaction to risky events.

(a) IT related loopholes are to be communicated in timely fashion to right forum at right time for right response.
(b) Immediate gain/loss/opportunities from IT related events are to be exploited.
(c) Communicating IT risk analysis result.
(d) Reporting risk management activities and compliances.
(e) Independent IT assessments are to be interpreted.
(f) Identifying IT related opportunities.
(g) Intimating/maintaining incident response plan.

Monitoring IT risk management ensures optimizing & integrating day to day operations with overall IT risk strategy and business decisions.

(a) Fixing personal or individual accountability for IT risk management.
(b) Harmonizing business & IT risk strategy.
(c) Integrating IT risk practices to enterprise risk practice.
(d) Risk based transaction monitoring surveillance process should be kept in place.
(e) Optimizing resource allocation for IT risk management
(f) Independent risk assurance for IT risk management.
(g) A suitable framework for Business Continuity Management may be implemented.

## VII. CALCULATING COMPLIANCE METRIC

In this section, we will show how risk assessment metric can be calculated for CobiT (Fig. 3) to arrive at the compliance measurement. In this tree structure, each node represents weight $w_i$ which measures relative contribution of each event to the overall event assessing risk. Now, specific weight distribution is beyond the scope of this paper, but nominally they are proportional to fraction of total man-hour an auditor spends in auditing each task. It is arrived after extensive consultation with a number of information system auditors who are engaged in calculating relative weight distribution in risk management of an enterprise undergoing Information Security Compliance. One auditor, while checking for an organization claiming to be CobiT compliant, may first want to verify whether identification of strategic and tactical risk to be .2 and .05, respectively making risk portfolio to be .25 out of .35. The auditor may also give historical risk trends and events to be .1 making categorizing risk to be .35 out of possible .5. The auditor also gives identification of internal/external context of risk assessment a value equal to .15 out of .2.

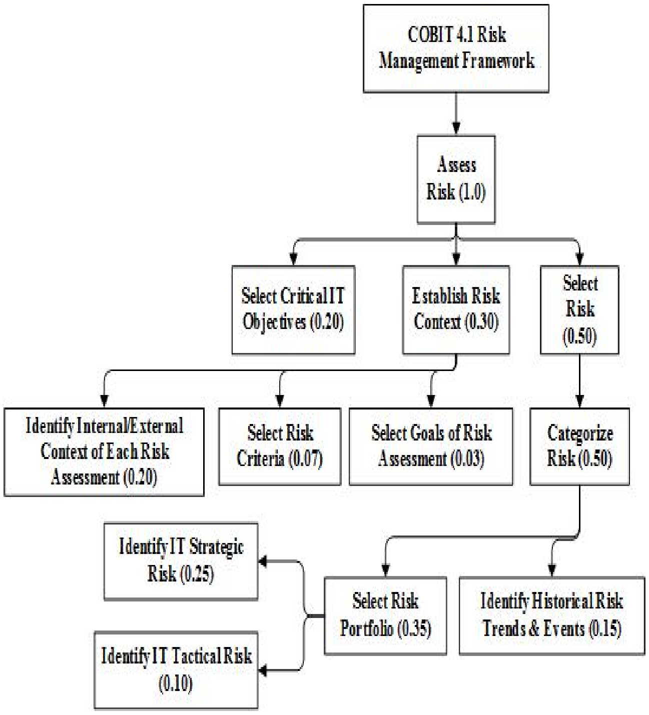
COBIT 4.1 Risk Management Framework
Assess Risk (1.0)
Select Critical IT Objectives (0.20)
Establish Risk Context (0.30)
Select Risk (0.50)
Identify Internal/External Context of Each Risk Assessment (0.20)
Select Risk Criteria (0.07)
Select Goals of Risk Assessment (0.03)
Categorize Risk (0.50)
Identify IT Strategic Risk (0.25)
Select Risk Portfolio (0.35)
Identify Historical Risk Trends & Events (0.15)
Identify IT Tactical Risk (0.10)

Figure 3. Assessing Risk (CobiT 4.1)

Selecting risk criteria to be .05 and goals of risk assessment to be .01 makes establishing risk context to be .21 out of possible .3 . The auditor also selects critical IT objectives to be .15 out of .2. It makes assessing risk to be .71 (.35+.21+.15). Normally, it passes for unqualified opinion from the auditor. In this case, some most critical observation regarding weight distribution and corresponding evaluation by the auditor may not be out of place. Primarily, two most important cases arise as follows:

(a) Perfect Organization: here, the auditor is satisfied about the procedures followed and data maintained in the organization's database and opine that the organization is following the regulation, and gives an unqualified opinion.

(b) Imperfect Organization: here, the data and procedure maintained by organization leaves much to be desired as per auditing standard. Following sub-cases may arise:

(i) Qualified opinion: the auditor gives an opinion on the organization performance and up-keeping of data and records and methodology used in auditing process ( subject to certain reservations).

(ii) Adverse (Negative) opinion: the auditor determines that he does not agree with the affirmations to be made by the respective organization. Based upon the material facts he may give an adverse opinion on the conduct of the business, resulting in legal, financial problems for the organization.

(iii) Disclaimer of opinions: when an auditor fails to obtain sufficient appropriate audit evidence to warrant an expression of opinion either on the conduct or on the procedure of the business, the auditor may make a disclaimer of opinion on the said organization.

(iv)Piecemeal opinion: such an opinion may be given in case when the auditor concludes that he is hereby unable to give an overall opinion on the statements and procedure of the organization but he can express an opinion limited to certain portion of the audit report of the organization.

In our example, the auditor may give unqualified opinion as the bank compliance touches 71%.

## VIII. CONCLUSION AND FUTURE WORK

In this paper, we proposed an ontology based model for a particular standard (Cobit4.1) in information security domain in Indian banking sector. We will conclude by briefly stating some limitations of our work. While calculating compliance, proper attention was not paid about organization (bank) groupings, culture and size. Due to space constraints, designing architecture of agents performing compliance auditing as well as real life cases involving missing/incomplete/ambiguous data could not be undertaken. For future direction of our research, completeness, redundancy and consistency of analysis of information security model may be undertaken in a formal manner and the comparative studies between different security standards may be investigated in multiple domains.

## REFERENCES

[1] A. D. Preece, "A new approach to detecting missing knowledge in expert system rule bases", International Journal of Man-Machine Studies, Vol. 38, No. 4, pp. 661-668, April, 1993.

[2] A. Gangemi, "Ontology Design Patterns for Semantic Web Content", In Proceedings of the 4th International Semantic Web Conference (ISWC), pp. 262-276, 2005.

[3] A. Gómez-Pérez, L. M. Fernández, and O. Corcho, "Ontological Engineering with examples from the areas of knowledge management, e-commerce and the semantic web", London: Springer, 2004.

[4] E. Sanchez, "Fuzzy Logic and the Semantic Web", Elsevier, 2006.

[5] G. Lau, K. H. Law, and G. Wiederhold, "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.

[6] J. Li, "Robust Rule-Based Prediction", IEEE Txn on Knowledge and Data Eng. Vol 18, No. 8, August 2006.

[7] L. Zadeh, "Fuzzy Sets", Information and Control, Vol. 8, pp. 338-353.

[8] Managesoft, "Managesoft Compliance Manager", (http:// managesoft-compliance-manager.software.informer.com) (Last access 17/3/13)

[9] SEC, "Sarbanes Oxley Act 2002", U.S. Securities and Exchange Commission.

[10] Symantec, "Improving IT Compliance: Guidance for Midsize Organizations", Whitepaper, July, 2006.

[11] S. Ammar, R. Wright, and S. Selden, "Ranking State Financial Management: A Multilevel Fuzzy Rule-based System", Decision Sciences 31 (2), pp. 449-482, 2000.

[12] US Dept of Health and Human Services, "Health Insurance Portability and Accountability Act (HIPAA)",1996.

[13] W. Siler and J. J. Buckley, "Fuzzy Expert Systems and Fuzzy Reasoning", John Wiley & Sons, Inc, 2005.

[14] Indian Banking Fraud Survey-2012- Navigating the Challenging Environment (Deloitte February 2012).

[15] Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds (RBI, January 2011) (http://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WREB210111.pdf) (Last access 17/3/13).

[16] P. Saha, N. Parameswaran, B.B. Chakraborty, and A. Mahanti" A Formal Analysis of Fraud in Banking Sector" 46th Hawaii International Conference On System Sciences (7-10 January, 2013 Wailea, Maui, HI 96753, USA).

[17] AS/NZS ISO/IEC 17799:2006 Information Technology — Security Techniques — Code of Practice for Information security Management (July 2006).

[18] Ernst & Young's 2012 Global Information Security Survey (http://www.ey.com/Publication/vwLUAssets/Fighting_to_close_the_gap:_2012_Global_Information_Security_Survey/$FILE/2012_Global_Information_Security_Survey___Fighting_to_close_the_gap.pdf) (Last access 17/3/13).

[19] A. Hevner, S. March, J. Park, and S. Ram (2004). "Design Science in Information Systems Research", MIS Quarterly, Vol. 28, No. 1, pp. 75-105.

[20] IT Governance Institute: Control Objectives for Information and Related Technologies (COBIT) (www.itgi.org) (Last access 17/3/13)

[21] Bank for International Settlement (2011) "Basel III: A Global Regulatory Framework for more Resilient Banks and Banking Systems" (www.bis.org ) (Last access 17/3/13)

[22] N. K. Cicekli and Y. Yildirim "Formalizing Workflows Using the Event Calculus". Database and Expert Systems Applications, Springer 2000.

[23] K. F. Brickey, "From Enron to Worldcom and Beyond: Life and Crime after Sarbanes-Oxley", Washington University Law Quarterly Vol. 81, pp. 357-401, 2003.