Compliance Management Model for Interoperability Faults towards Enhanced COBIT Governance of Enterprise Software

KANCHANA NATARAJAN
Department of Computer Science
Bharathiar University
Coimbatore, TN, INDIA
kanchananatarajan@live.com

Abstract: - A quantitative and analytical approach is essential to explore the impact of risks on the enterprise due to interoperability in the case of multi-software activation process. The main objective of the research is to propose a software compliance management model for interoperability fault of regulatory non-compliances in IT industries towards better quality governance. The entities that are non-adherence to the standards and failed to follow the enumerated regulations are analyzed for the non-compliances. The non-compliances in procedure-oriented processes and coding are mapped with the risks associated with severity and impact on the chosen applications. The interoperability fault due to non-compliances are identified and detected much earlier to have a better governance and minimal risk. The interoperability faults within the COBIT (Control Objectives for Information and Related Technology) framework are considered to detect and categorize the injected faults towards the enhancement of governance of the system while considering the non-compliances during compilation of an application. The conformance to the requirement specifications pertaining to process, people, product and its quality are verified as a distributed system to manage the non-compliances. The existing information governance can be improvised by the proposed Governance Enhancement Technology (GET) with the help of a case study on healthcare management system with deployed web services. This research work exhibits the integration of IT compliance with the risk management through the risk of non-compliance.

Key-words: - Business Risks, Non-Compliances, COBIT Compliance, Interoperability Fault, Verification Standards, Goal-risk model

1 Introduction

The IT industry exhibits a steady and positive growth over a decade and at the same time the non compliances in different developmental phases with different forms are increasing. This trend will lead to a major crisis in the IT business sector since the corporate are having global perspective. An international business over IT related products like licensing, design, security and consulting solutions become services with on-demand accounting and auditing. The three different disciplines like technical wing, legal wing and administration wing have to coordinate and collaborate not only to procure any software related products such as intellectual properties but also market the same to satisfy the customers. Meanwhile, the various issues and challenges in the governance of non-compliances can solve through the structured management technique called Regulatory Compliance Management (RCM). It ensures that the data, processes and organization are structured in accordance with the regulations of the guidelines which are specified in the regulations [1].

1.1 Software Compliance

Software compliance is defined as a 'state of conformance to the requirements based on standards of the respective domain'. The semantics and scope of compliance become increasingly complex due to the large number of regulations and standards that are introduced by the local or global policy makers. The regulations are to be followed in order to meet out the prescribed standards in the requirement elicitation. The documentation and maintenance agreement also comes under regulatory activities which are vulnerable if not having met the enforcement acts [2]. To identify the exact interoperability faults in any software the development and management teams have to be trained with the existing standards and compliances across the domain of interest. The cost of non-compliances is more expensive which can be reduced when the organization initially spends a higher proportion of IT budgets on compliance activities especially on the factors of global privacy, regulatory constraints and legal obligations [3].

1.2 Software Non-Compliance and Interoperability Faults

The necessity of the process model should have control to monitor the compliance constraints through reviews and audits to avoid the risk of non-compliance and financial penalty's [4]. The non-compliance may also lead to risks of legal sanctions or customer trust loss due to inadequate services of the software product. The issues may evolve in terms of the failure of compliance features which includes complexity, reusability, understandability and maintainability [5]. Especially to fulfill the control objectives it is needed to have a correct and timely composition of services which depends on the quality features and associated quality attributes [6] [7]. One among the quality sub-attributes of ISO/IEC 25010-1 standard for software quality model is interoperability, states that regulations to handle the capability of the software product to interact with one or more specified systems. The interoperability faults in the software processes may begin in the lower level of implementation were each and every quality feature has to be ascertained in all possible combinations to assure the expected system behavior [8, 33]. Hence, interoperability has been defined as the ability of two or more systems to exchange information and to use the information that has exchanged [12].

1.3 Corporate Scandals and Compliance Resources

The software compliance resources usually instruct to follow the best business practices to ensure and sustain the high-level objectives. The analysis of non-observed measurement factors through best practices may solve the issues of non-compliances [9]. The corporate issues include 2G Scam, WorldCom and Enron [13] which are based on auditing applications due to the failed applicable regulations and accountability acts. An ontology-based information model of COBIT 4.1 risk management framework ensures the compliance of banking sectors by ensuring do the information security standards like COBIT, HIPAA [1,2,12], SOX [2,4,12], PCI DSS [3] and BASEL III [5] are followed [10]. A scrum-based software development process measurement using COBIT criteria assess the levels of compliances. The authors revealed that the non-compliant indicator does not depend on the software development method but related to the human resources strategy and project management strategy on the organizational level [11].

2 Review of related works

Existing research on interoperability models ensures the compatibility and integration level of large scale systems through Capability Maturity Model Integration (CMMI), Government Interoperability Maturity Matrix (GIMM) and Business Interoperability Quotient Measurement Model (BIQMM) [12]. The lack of applicable domain-specific models for small scale systems arise several non-compliances thereby the research inter-relates interoperability and compliance in the context of standards of the domain. There are many solutions for the problem of modeling and checking compliance, as well as violation recovery through meta-model by defining syntax, semantics and notations. The scale and diversity of compliance requirements are changing with respect to many features like application criticality, deployment platform, modes of control and its selectivity of domain specific problems which may change more frequently. Such large and complex problems necessitate a formal representation of control objectives in Formal Contract Language (FCL) or Process Compliance Language (PCL) [13], the languages which are suitable to capture the declarative nature of compliance requirements [14]. The commitment, privilege and right analysis [15] and its effectiveness of requirement engineers involved in the extraction of compliance requirements from privacy policy which results much better in the view of correctness and completeness.

The conceptual approach for the regulatory compliance issue [16] has the combination of an organization’s business process management on the one hand and a respective accompanying meta-model covering risk and control mechanisms for achieving compliance on the other. The regulatory compliance framework [17] have been integrated with set of software requirements and regulations as input to identify the irregularities there by associating argumentation tree structure in order to capture the arguments to ensure its acceptability. Hence the framework is subjective used only under certain circumstance which shows the evidence for framework’s inadequacy. The limitation of this model implies the coverage and failure of pattern to specify compliance requirements at certain instances may increase the compliance risk [18]. The rule-based compliance checking is considered to common businesses which reveal the compliance failures of designed process models. It also identifies and assesses the potential compliance risks along with its information [19]. The risk assessment framework ensures safety and security fields of software domain based such as Functional Hazard Assessment (FHA), Preliminary Hazard Analysis (PHA), HAZard and OPerability (HAZOP), Failure Mode and Effect Analysis (FMEA), Fault Tree Analysis (FTA), Knowledge Acquisition in Automated Specification-Security Extension (KAOS SE) and Secure Tropos [20]. Automatic process-oriented governance and compliance maturity model (GoCOMM) refines the business process and regulatory bodies to enhance the measurable goals of compliance and security. The model defines five levels of maturity with the base of correlation between control and objectives, automation and measurements [21]. The regulatory compliances between business processes with polynomial time which is based on the intersection of non-monotonic deontic logic and formal semantic annotation that ensures the logical state gaps to diagnose information which results in guaranteed detection of any obligations and compliance gaps during the execution time [22].

Distributed Online Rule Analysis (DORA) algorithm coordinates the exchange of information across monitoring servers for obtaining a complete assessment of the policy violations present in the infrastructure with certification evidence [23]. The process compliance model focused the development of demonstrable methods to derive control tags, heuristics, improved process annotation and analysis through the notion of compliance distance for process analysis [24]. Alexander Davis et al. analyzed the application development by comparison of SOAP and DCOM technologies in terms of efforts during development and performance with the use of same AMSDB database. The Simple Object Access Protocol (SOAP) [34] is a multi-platform technology has been solely adopted for increasing interoperability of web service applications but lacks with the feature of security management. While the Distributed Component Object Model (DCOM) is a single-platform technology which supports security aspects but lacks with the features of interoperability and scalability [25]. Interoperability Classification Framework for enterprise application classifies the interoperability problems with different set of dimensions and develops a situation-specific structure of knowledge-based approach in method-chunk repository which is a reusable component [26]. The earlier research work of our contribution [31] discusses the framework along with its regulations of the proposed work. Along with it's the extension of this paper addresses the various software component services and executables in a distributed environment to collect process and report the available, traceable non compliances in the processes and also in the resources.

3 Governance Risk and Compliance Management in COBIT

The identification for the possibilities of integration of many high-level processes in three sectors such as IT governance, IT risk management and IT compliance is complex. It is necessary to examine the relation of the three sectors before merging them into a single integrated-process model through combinable processes [28]. The COBIT framework [32, 35] for IT and related technology can be considered as a set of entities that are associated with each other in a triangular manner. The control requirements have to address all the technical issues and challenges not only in monitoring but also in the operational phase of that business. The control requirements must consider the possible risks involved if they cannot meet the set of issues and requirements. A bidirectional association exists between the entities of the three different sets in a triangular manner for governance is shown in the fig. 1.

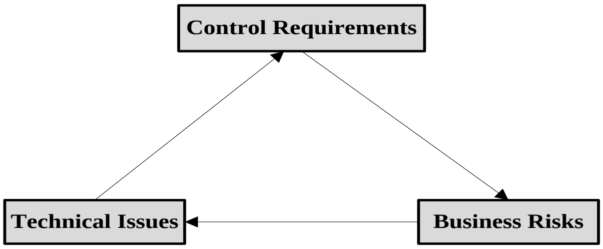


Fig. 1 Governance Association in COBIT

In order to ensure different forms of compliances the COBIT control requirements are classified into five categories such as people, product, process, quality and production control requirements. The non-compliances may evolve due to the reason of non-adherence of standards associated to the control requirements. These control requirements are to be satisfied based on the business processes, products, procedures and people. The non-availability of safety critical applications and the low maintainability of the industrial process control software will increase the probability of major risks in the production and human loss. Risk exposure element determines the priority and organization of quality requirements in all commercial software. The focus of all these analysis and study is to minimize the impact of risks at all levels [29] [30].

4 Computational Model for Interoperability Faults towards Enhanced Governance

The proposed computational model focuses the detailed association of the control requirements with all technical issues which leads to different forms of business risks. Commonly, risk can be expressed as $R = P \times I$, where R is the project risk exposure, P is the probability of the risk factor's occurrence, and I is the impact of the risk factor. Generally risk can be quantitatively expressed as in the equation (1) & (2) is shown below. The number of instances or occurrences of non-compliance in that domain are due to the control requirements in the processes. The interoperability faults are the hazards in the processes and in the resources and they become the defects in the case of people and devices depend on the faults and their impact levels. The fig.2 indicates the technical issues that are being transformed as control requirements due to all these types of interoperability faults along with the variations in the policies and business guidelines or standards. The compliance management is distributed across all the domains, processes and resources along with the policies. The individual player in the overall governance through compliance management can be illustrated through mathematical relationships and their integration across the framework. The proposed approach, the GET is considered as a net list of functions and their sub functions through functional programming. Instantly, it is quite an evidence in declaring the governance of enhanced technology, let $\mathrm{GET}_{\mathrm{COBIT}}$ as a domain of number of processes which needs different information about a variety of resources can be written as *Domain (Process (Information (Resources)))*.

$$\text{Risk} = \sum_{i=1}^{n} P\,(NC) * [1 - P\,(\text{Defect in Resources} * \text{Hazard Level in Processes})] \qquad (1)$$

$$\text{Business Risk} = \text{Total Instance of Non} - \text{Compliance} * \left[1 - \text{Probability}\left(\text{IOF}(\text{Resources})\right).\left(\text{IOF}(\text{Processes})\right) * \text{Probability}(\text{Technical Issues})\right] \qquad (2)$$

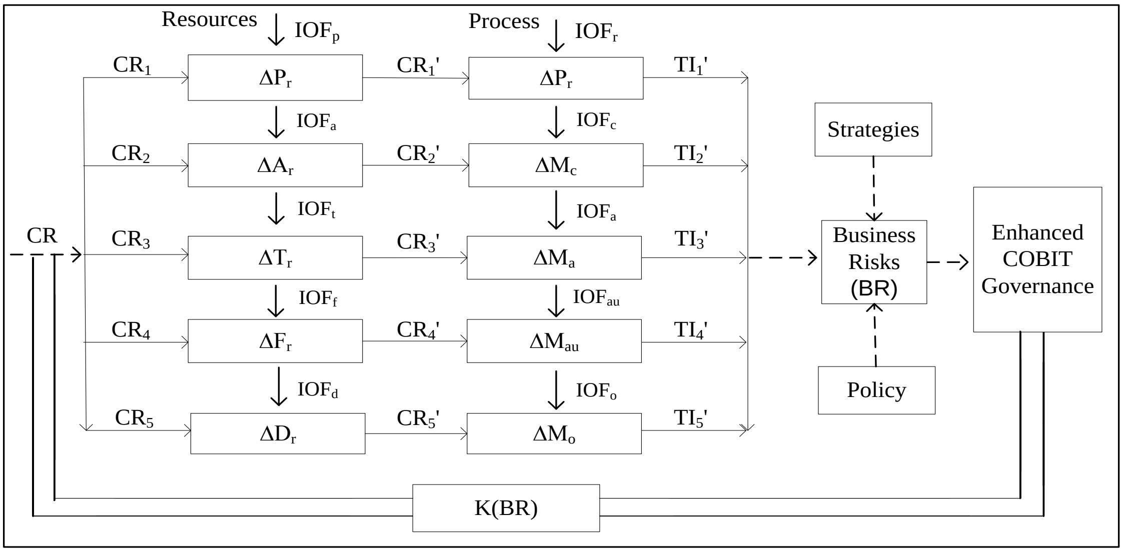


Fig. 2 Flow Diagram of Business Clocked Feedback Control for Enhanced Governance

Table 1: Enhanced Governance by Compliance Management Entities (Process & Resources)

DOMAIN		PROCESS	INFORMATION CRITERIA	IT RESOURCES				
			Compliance	People	Applications	Technology	Facilities	Data
Planning & Organization								
	PO6	Communicate Management Aims & Direction	S	1	0	0	0	0
	PO8	Ensure Compliance with External Requirements	P	1	1	0	0	1
	PO9	Assess Risks	S	1	1	1	1	1
Acquisition & Implementation								
	AI2	Acquire and Maintain Application Software	S	0	1	0	0	0
	AI4	Develop and Maintain Procedures	S	1	1	1	1	0
Delivery & Support								
	DS1	Define and Manage Service Levels	S	1	1	1	1	1
	DS2	Manage Third-Party Services	S	1	1	1	1	1
	DS5	Ensure Systems Security	S	1	1	1	1	1
Monitoring								
	M1	Monitor the Processes	S	1	1	1	1	1
	M2	Assess Internal Control Adequacy	P	1	1	1	1	1
	M3	Obtain Independent Assurance	P	1	1	1	1	1
	M4	Provide for Independent Audit	P	1	1	1	1	1

Table 2: Representation of Governance Requirements

GET_p *= Planning (Compliance (External Requirements (People))) +Monitoring (Compliance (Internal Control Adequacy (People))) +Monitoring (Compliance (Independent Assurance (People))) +Monitoring (Compliance (Independent Audit (People))) (1)*

Similar logical expression can also be written as follows:

GET_a *= Planning (Compliance (External Requirements (Applications)))+ Monitoring (Compliance (Internal Control Adequacy (Applications)))+ Monitoring (Compliance (Independent Assurance (Applications))) +Monitoring (Compliance (Independent Audit (Applications))) (2)*

GET_t *= Monitoring (Compliance (Internal Control Adequacy(Technology))) + Monitoring (Compliance (IndependentAssurance(Technology)))+Monitoring(Compliance(IndependentAudit(Technology))) (3)*

GET_f *= Monitoring (Compliance (Internal Control Adequacy(Facilities))) + Monitoring (Compliance (Independent Assurance(Facilities))) + Monitoring (Compliance (Independent Audit (Facilities))) (4)*

GET_d *= Planning (Compliance (External Requirements (Data))) +Monitoring (Compliance (Internal Control Adequacy (Data))) +Monitoring (Compliance (Independent Assurance (Data))) + Monitoring(Compliance (IndependentAudit(Data))) (5)*

The table 1 shows the compliance management entities of processes and resources in the application domain. The primary and secondary compliance resources of processes of the domain are listed based on the COBIT framework in order to enhance governance. Hence the governance can also be represented in the form of compliance requirements as an internal and external processes uses training and monitoring towards auditing. The governance requirements can be represented as a chain of functions is shown in the table 2.

The early detection of non-compliances like the interoperability fault is considered as a requirement fault. It is possible only with the above enhanced model where the governance can be calculated in terms of the integrated value of the ratio of control requirement factors encompassing all resources to the total technical issues towards possible interoperability features and business risks. The quantitative analytical representation can be given as in the equation mode (3) & (4) is shown below,

$$GET_{COBIT} = \sum_{i,j}^{m,n} \frac{CR_i(P + A + T + F + D)}{TI_j(\ P_r + M_c + M_a +\ M_{au} + M_o)}(IOF_i + BR_j) \qquad (3)$$

Interoperability (IO) Faults are in the processes and resources which are essential to achieve the governance over the framework. The quantification of these faults depends on the individual process handling and resource utilization. The technical issues and business risks are arising due to improper handling of the above mentioned processes and their respective resources.

$$GET = CR - (K * BR) = \sum\left(\frac{CR1^{'} - CR1}{IOr} * \Delta R + \frac{TI1^{'} - CR1'}{IOp} * \Delta P\right) \qquad (4)$$

5 Procedural and Regulatory Compliance with COBIT Framework

To ensure procedural and regulatory compliances in the domain of planning and organization of requirements process within the COBIT Framework, the resources such as people, application, technology, facilities and data are considered as the critical factors for non-compliances. By effectively focusing these resources the organizations can save the time, costs and efforts with higher quality and productivity. The improved governance for regulatory and procedural non-compliances is focused with application level. The non-compliances have direct impact on stakeholder's need while compliance becomes a major requirement for every organization they must be able to demonstrate as well. The non-compliances such as procedural, regulatory, reliability and people are non-adherence to the standards of the application code. The financial risk arises due to the procedural non-compliance on client program which leads to the non-completeness of the application code. Similarly the maintenance risk, process risk and reputation risk arises due to the regulatory non-compliance, reliability non-compliance and people non-compliance on query program, server third-party program and application program leads to the non-orderliness, non-availability and non-correctness of the application code. As shown in the first row of the table 3, the COBIT 5 framework has followed by the requirement team of IT industries in the entity level of planning.

The relation or associations involved in the external requirement process are non-compliant due to people, application, data but the resources are not permitted with adherence to COBIT 5 regulation. This non-permissible compliance fault due to interoperable resources within the framework can be represented as CR=P'+A'+T+F+D'. The compensation factor represented as k, the Compensation Factor (CF) and represented as a tuple as,

$$G_{IT} = \langle \text{Confidence, Customization, Control} \rangle$$

The expected Governance Enhanced Technology (GET) covers three different set of entities, Control Requirements (CR), Technical Issues (TI), and Business Risks (BR). The time dependent governance enhancement can be represented as $GET_{COBIT}(t)$. The quantitative perspective makes the multi-set that represents the amount of difference between the actual and the desired or legal parameters, the degree of non compliance or the compliance violation and the amount of risk to be remediated. The governance within the framework can be enhanced by maximizing the compliance management in the gap for a fixed business risk and minimize the risk with varying technical issues from time to time for a fixed control requirement. Mathematically these compliance management metrics can be written as follows:

$$GET_{COBIT}(t) = \left\{ \begin{matrix} \text{Gap Violation} \\ \text{Compliance Violation} \\ \text{Risk Remediation} \end{matrix} \right\} = \langle G, C, R \rangle$$

$$\text{Non} - \text{Compliance Management Gap} = \frac{\Delta CR}{\Delta TI} \mid BR = \text{Fixed}$$

$$\text{Minimize Risk} = \frac{\Delta BR}{\Delta TI} \mid CR = \text{Fixed}$$

Table 3: Risk due to non-compliance and interoperability faults

COBIT 5 Framework	IT Team	Compliance Entity Level	Compliance Relation	Non Compliant Regulation/ Procedural	Compliant Requirement	Risk	
						Severity	% of Occurrence Frequency
CBT 1 Primary	Requirement Team	Plan	External Requirements Processes	May be Permitted	P'+A'+T+F+D'	0.45	Often
CBT 2 Primary	Analysis Team	Monitor	Internal Control Processes	Permitted	P'+A'+T'+F'+D'	0.51	Medium
CBT 3 Secondary	System Testing Team	Plan	Management Processes	Not Permitted	P'+A+T+F+D	0.58	Medium
CBT4 Secondary	QA Team	Organize	Assess Risks Processes	Permitted	P'+A'+T'+F'+D'	0.66	Always
CBT5 Secondary	Web Deployment Team	Acquire	Maintain Procedures Processes	Permitted	P'+A'+T'+F'+D'	0.77	Never
CBT6 Secondary	Quality Control Team	Deliver	Systems Security Processes	Permitted	P'+A'+T'+F'+D'	0.34	Low

The better governance concentrates the compliance gaps, adequately justifies risk acceptance, reacting quickly to changing laws, evolving regulations and sometimes through overlapping standards. The other way of overcoming the non compliances is to mitigate and manage them as per the guidelines given in the standards. The serious issue in risk management is to identify the risks as risks not as faults. There are occasions where a fault may not turn into serious business risk and vice versa. The risk management must concentrate on the concern about the risk and its counteraction on the business setup. The non-compliance in critical entities like mandatory requirement like licensing and storage may lead to potential damage not only to the production but also to the reputation of the company.

6 Case Study

INTEROPERABILITY DRIVEN DISTRIBUTED HEALTHCARE MANAGEMENT SYSTEM:

The case study on Healthcare Management System describes how the different naming conventions between J2EE technology and .NET can cause difficulty in Web services interoperability. In both J2EE technology and .NET, it is quite common to share XSD schemas among multiple Web services. In fact, it is one of the best practices to share XML schemas for the purpose of modular design and reusability. The XML tag: import and include, are used just for this purpose. Below XML block is a Medicine element which is being used by web services. Medicine element is developed under .NET technology which is being used by multiple web services under HM application.

```
<?xml version="1.0" encoding="UTF-8"?>
<schema
xmlns="http://www.w3.org/2001/XMLSchema"
targetNamespace=
"http://medicine.warehouse.com"
xmlns:Product="http://medicine.warehouse.com">
<complexType name="Medicine">
<sequence>
<element name="_int" type="int"></element>
<element name="_name" type="string"></element>
</sequence>
</complexType>
</schema>
```

Since every element should be packaged under one namespace, hence it's been packaged under http://medicine.warehouse.com. This package will be integrated with other web services during communication between web application and web services. Medicine element provides list of medicine's available. Medicine, Order and Inventory element are integrated and available inside the same namespace to communicate between the elements. Inventory element denotes the total availability of the medicine. Whereas order element are integrated with medicine element whenever it goes out of stock. Meanwhile Order element is integrated with Inventory element based on the minimum stock availability of the medicines.

Inventory Service developed in .Net technology

```
[WebService(Namespace="http://inventory.warehouse.com/service")]
public class InventoryProductService:
System.Web.Services.WebService
{
[WebMethod]
[XmlInclude(typeof(Medicine))]
public string RestockProducts(Medicine[] medicine)
{
// .Net code to process the inventory service
}
}
```

Order Service developed in .Net

```
[WebService(Namespace="http://order.warehouse.com
/service")]
public class OrderProductService:
System.Web.Services.WebService
{
[WebMethod]
[XmlInclude(typeof(Medicine))]
public string OrderProducts(Medicine[] medicine)
{
// .Net code to process the order service
}
}
```

The above two web services are deployed in the Internet Information service (IIS) which can be used by any interfaces. Web Services Description Language (WSDL) has to be generated from the above web services, which can be integrated with J2EE application. WSDL describes a Web service. It specifies the location of the service and the operations (or methods) the service exposes. An RPC-based Web service is a collection of procedures that can be called by a remote client over the Internet. WSDL from .NET web service will be used in J2EE application for integration using JAX-RPC. With JAX-RPC, client written in a language other than the Java can access a Web service developed and deployed on the Java platform. Meanwhile, a client written in the Java can communicate with a service that was developed and deployed using other platform.

Interoperability is possible with JAX-RPC though support of SOAP and WSDL. SOAP has its own standards for XML messaging, so any applications following the standards will communicate each other. The SOAP specification defines the envelope structure, encoding rules, and conventions for representing remote procedure calls and responses. These calls and responses are transmitted as SOAP messages (XML files) over HTTP. Below shown the XML generated from the order web service during the SOAP request from J2EE application.

```
soapenv:Body>
    <OrderProduct
xmlns="http://order.warehouse.com/service">
        <products>
            <Product>
                <_name
xmlns="http://medicine.warehouse.com">Medicine1</_na
me>
                <_qty
xmlns="http://medicine.warehouse.com">10</_qty>
            </Product>
            <Product>
                <_name
xmlns="http://medicine.warehouse.com">Medicine2</_na
me>
                <_qty
xmlns="http://medicine.warehouse.com">20</_qty>
            </Product>
        </products>
    </OrderProduct>
</soapenv:Body>
```

Above are the XML generated from the inventory web service during the SOAP request from J2EE application. By comparing the two SOAP requests, Order service has a direct reference to Medicine type whereas inventory service doesn't have a direct reference indeed it has a reference through Order web service. During integration of .Net web services, JAX-RPC creates distinct directory structure for both Inventory and Order services. Medicine type service has been created under the directory com.order.warehouse.service which is part of order web service classes. But for Inventory service, Medicine type service is not created.

During .Net web service development, both web Order and Inventory web service has a direct reference to Medicine to get it interconnected. But when we deploy the same services with native technology, both web services are created with own packages but the reference between the elements are broken. For instance, list of unavailable medicines were transferred to Order web service for placing the order which will place the information in the database by using .Net web service. But when we try to fetch the list of inventory, it returns empty because the element Medicine and Inventory references are broken while integration and the Medicine element used in the inventory service is associated with Order service.

```
<soapenv:Body>
    <RestockProduct
xmlns="http://inventory.warehouse.com/service">
        <products>
            <Product xmlns="http://order.warehouse.com/service">
                <_name
xmlns="http://medicine.warehouse.com">Medicine1</_name>
                <_qty
xmlns="http://medicine.warehouse.com">10</_qty>
            </Product>
            <Product xmlns="http://order.warehouse.com/service">
                <_name
xmlns="http://medicine.warehouse.com">Medicine2</_name>
                <_qty
xmlns="http://medicine.warehouse.com">20</_qty>
            </Product>
        </products>
    </RestockProduct>
</soapenv:Body>
```

Hence the .Net web service fails to perform interoperability with J2EE application. The verification form shown in fig. 4 illustrates the type of application and services chosen with the healthcare management system. The number of modules in the distributed system is listed along with the header files used for each module. The input standard declaration is also categorized here as variable, document and interfaces standards. Therefore the non-compliances and risks evolved in the application program, server third-party program, query program and client program are prioritized in order to differentiate the level, frequency and severity of risks.

7 Experimental Results

In the software perspective, the risk control objectives are to be identified with its associations. The proposed distributed compliance management architecture within the COBIT framework determines the possible business risks and their association with the technical issues. The control objectives must be redirected so as to define and declare the set of possible non-compliances found in the resources like either in the processes or in the people. The table 4 indicates the experimental values of GET which depicts the interoperability faults involved in the processes and resources.

There is no governance whereas the interoperability faults with control requirements, technical issues and business risks of resources and processes may varies with policies and guidelines. The triangular issues such as control requirements (CR1'), technical issues (TI1') and business risks (BR) can be evaluated by keeping the BR as constant.

Table 4: Experimental Values of Governance Enhancement Technology

CR1’	CR1	IOp	ΔR	TI1’	CR1’	IOr	ΔP	GET
0	0	0.1	0	0	0	0.6	0	0
0.25	0.2	0.3	0.2	0.25	0.25	0.2	0.3	0.03
0.5	0.4	0.4	0.3	0.5	0.5	0.1	0.4	0.15
0.75	0.6	0.2	0.6	0.75	0.75	0.4	0.7	0.67
1	1	0.6	0.8	1	1	0.5	0.9	0

The resources of facilities and processes of audit with respect to CR4’ rises rapidly were the governance improves by reduced business risks. In case of CR1’ and CR5’there is no governance were the resources of people and processes of review are with business risks as shown in fig. 3. The compliance relation associated within the COBIT framework and its severity level is represented in the fig. 5.

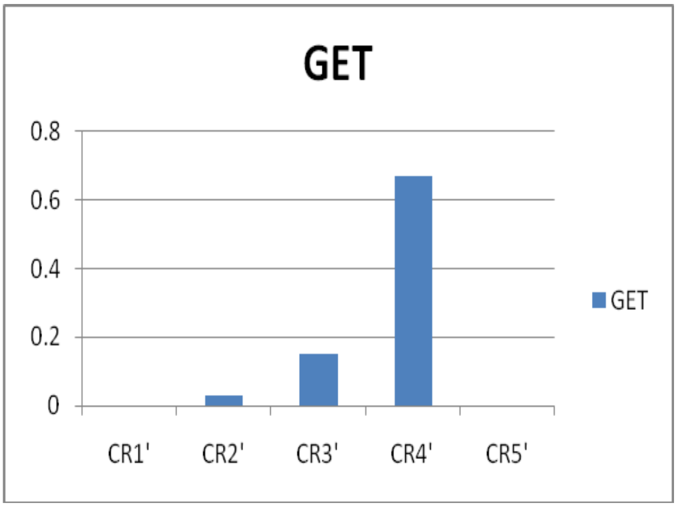


Fig. 3 Governance Enhancement Technology

The severity level is high in terms of Application Software Processes, Maintain Procedures Processes and Manage Service Processes. Hence, the Table 5 listed out the weightage of non-compliance checked against the defect rate and hazard levels which are scaled from 0 to 10 so as to ensure the impact and type of risks occurred in the Healthcare management application. The resources in the domain are considered to be facilities, application, technology, data and people.

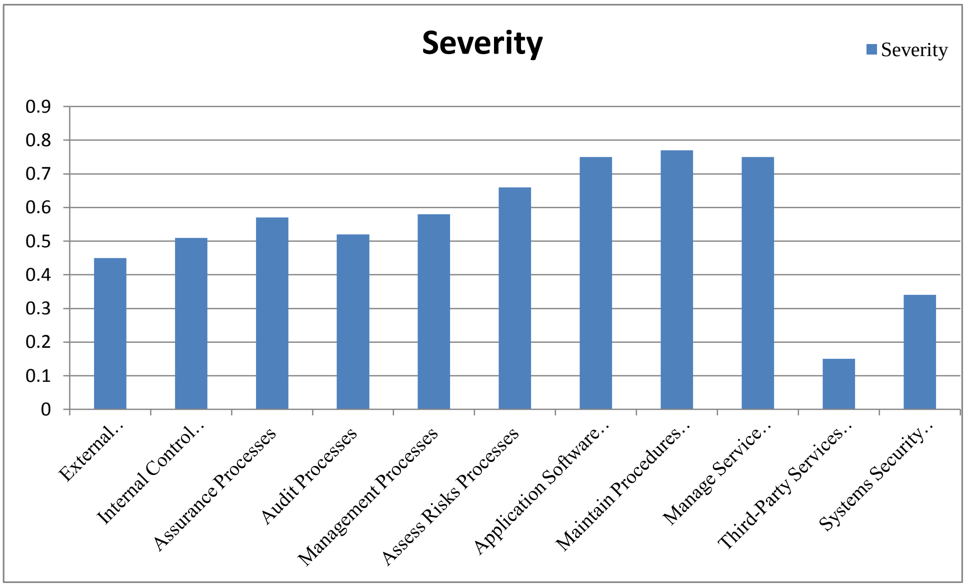
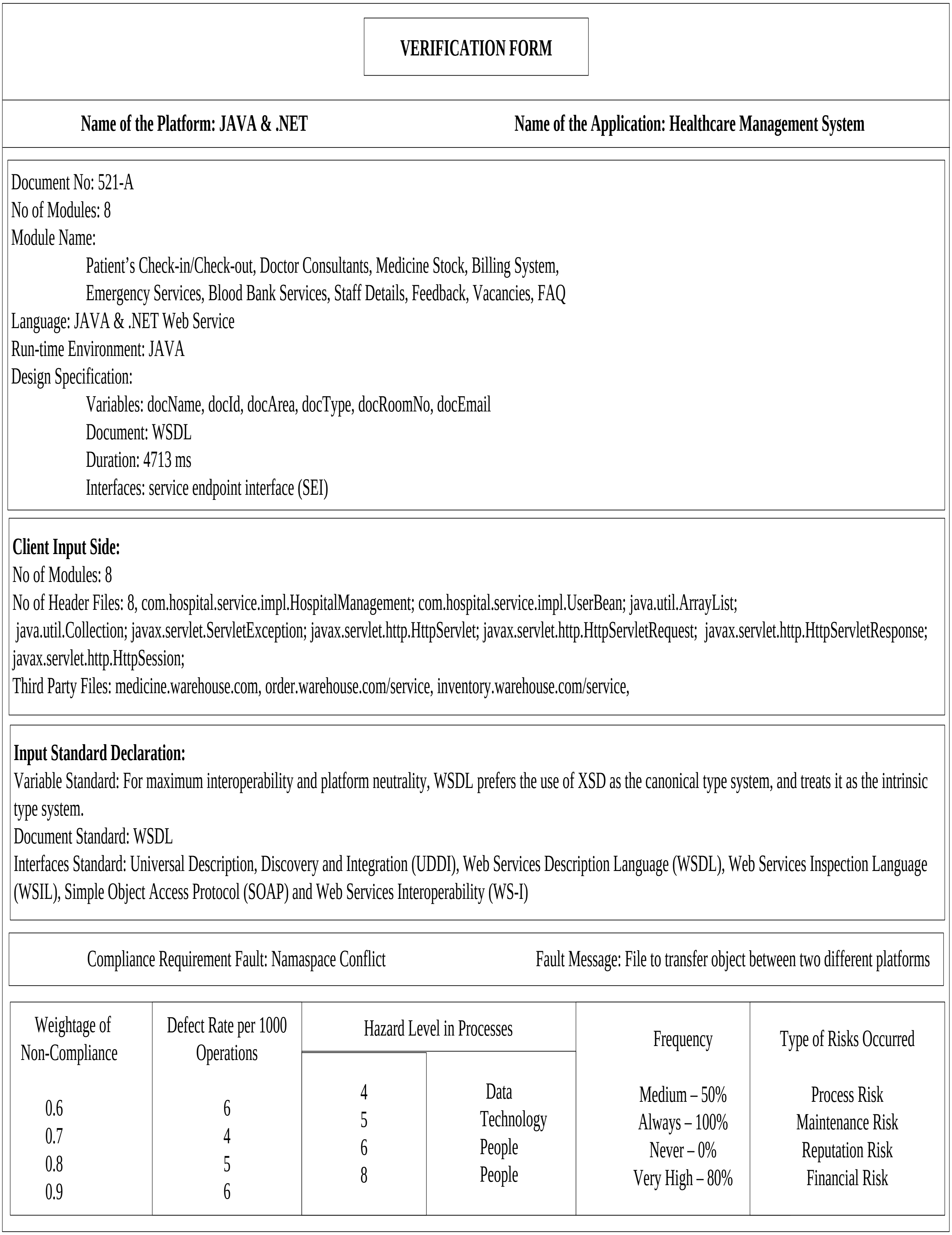


Fig. 5 Compliance Relation and its Severity



VERIFICATION FORM

Name of the Platform: JAVA & .NET **Name of the Application: Healthcare Management System**

Document No: 521-A
No of Modules: 8
Module Name:
Patient’s Check-in/Check-out, Doctor Consultants, Medicine Stock, Billing System,
Emergency Services, Blood Bank Services, Staff Details, Feedback, Vacancies, FAQ
Language: JAVA & .NET Web Service
Run-time Environment: JAVA
Design Specification:
Variables: docName, docId, docArea, docType, docRoomNo, docEmail
Document: WSDL
Duration: 4713 ms
Interfaces: service endpoint interface (SEI)

Client Input Side:
No of Modules: 8
No of Header Files: 8, com.hospital.service.impl.HospitalManagement; com.hospital.service.impl.UserBean; java.util.ArrayList; java.util.Collection; javax.servlet.ServletException; javax.servlet.http.HttpServlet; javax.servlet.http.HttpServletRequest; javax.servlet.http.HttpServletResponse; javax.servlet.http.HttpSession;
Third Party Files: medicine.warehouse.com, order.warehouse.com/service, inventory.warehouse.com/service,

Input Standard Declaration:
Variable Standard: For maximum interoperability and platform neutrality, WSDL prefers the use of XSD as the canonical type system, and treats it as the intrinsic type system.
Document Standard: WSDL
Interfaces Standard: Universal Description, Discovery and Integration (UDDI), Web Services Description Language (WSDL), Web Services Inspection Language (WSIL), Simple Object Access Protocol (SOAP) and Web Services Interoperability (WS-I)

Compliance Requirement Fault: Namaspace Conflict Fault Message: File to transfer object between two different platforms

Weightage of Non-Compliance	Defect Rate per 1000 Operations	Hazard Level in Processes		Frequency	Type of Risks Occurred
0.6	6	4	Data	Medium – 50%	Process Risk
0.7	4	5	Technology	Always – 100%	Maintenance Risk
0.8	5	6	People	Never – 0%	Reputation Risk
0.9	6	8	People	Very High – 80%	Financial Risk

Fig. 4 Verification Form of Compliance and Hazards

Table 5: Service table for non-compliances and risks

Weightage of Non-Compliance	Hazard Level	Impact	Resources	Type of Risk Occurred
0.6	2	Often – 90%	Facilities	Maintenance Risk
0.6	3	Medium – 50%	Application	Financial Risk
0.6	4	Medium – 50%	Data	Process Risk
0.7	2	Medium – 50%	Facilities	Maintenance Risk
0.7	3	Medium – 50%	Application	Financial Risk
0.7	5	Always - 100%	Technology	Maintenance Risk
0.8	8	High – 70%	People	Reputation Risk
0.8	6	Never – 0%	People	Reputation Risk
0.8	4	High – 70%	Data	Process Risk
0.9	6	Very Low – 10%	People	Reputation Risk
0.9	4	High – 70%	Data	Process Risk
0.9	8	Very High – 80%	People	Reputation Risk

Table 6: Experimental defect rate and hazard level in the Healthcare management system

Weightage of Non-Compliance	Defect Rate per 1000 Operations	Hazard Level in Resources		Impact
0.6	2	2	Facilities	Often – 90%
0.6	2	3	Application	Medium – 50%
0.6	6	4	Data	Medium – 50%
0.7	2	2	Facilities	Medium – 50%
0.7	2	3	Application	Medium – 50%
0.7	4	5	Technology	Always - 100%
0.8	2	8	People	High – 70%
0.8	5	6	People	Never – 0%
0.8	4	4	Data	High – 70%
0.9	2	6	People	Very Low – 10%
0.9	4	4	Data	High – 70%
0.9	6	8	People	Very High – 80%

The experimental result in Table 6 shows the defect rate per the number of operations and hazard level in the Healthcare management system with respect to the various resources and its impact. The weightage of non-compliance has been varying smoothly with respect to the number of iterations of the services. It is found that the defect rate varies abruptly in a pulsating manner among all iterations due to the different forms of interoperability faults across many processes and data. The defect rate varies with the increased number of iterations and it reaches high in the 3rd and 12th iterations which have shown in the fig. 6. Such situations may cause the specific type of non-compliance and its interoperability failure at those instances as per the application code. The weightage of non-compliance has been varying with increased rate with respect to the number of iterations of the services.

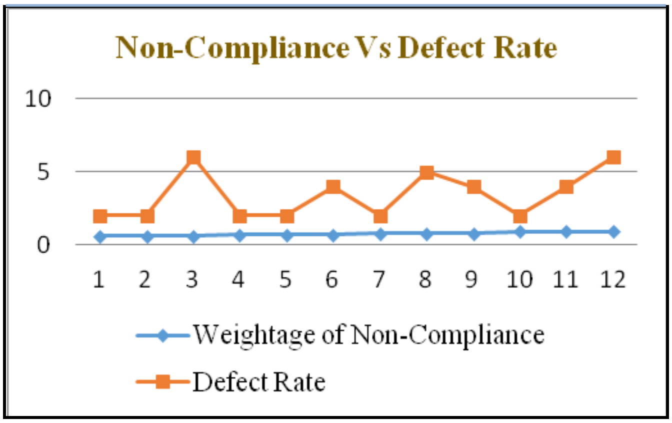


Fig. 6 Weightage of Non-Compliance Vs Defect Rate

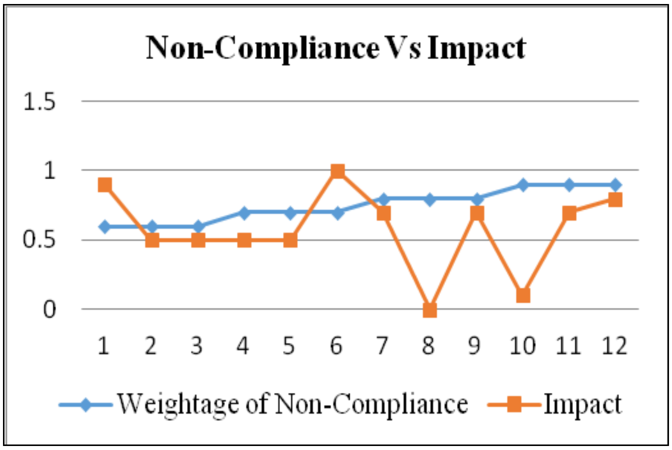


Fig. 7 Weightage of Non-Compliance Vs Impact

The fig. 7 illustrates the percentage of non-compliance raised during the process of application. The hazard levels in the resources are also determined against the impact of the non-compliances with the application in terms of number of operations as shown in the fig. 8. The hazard level rapidly increased with minimum levels and reaches the high level in the 7th iteration of the services which leads the type of non-compliance occurred also considered as an interoperability failure.

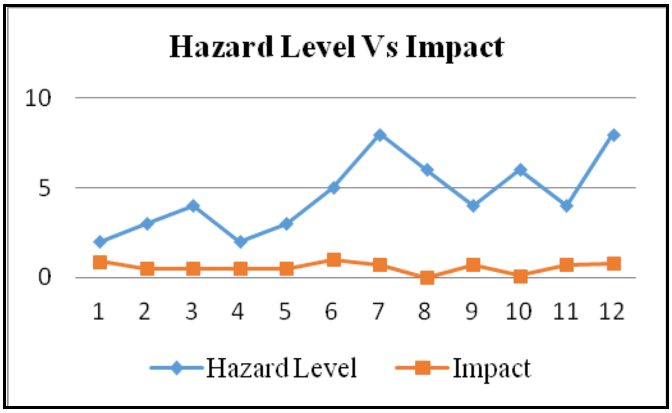


Fig. 8 Hazard Level Vs Impact

8 Conclusion And Future Works

The problem of achieving interoperability is closely related to standards of the applicable domain. The distributed software compliance management model focusing the interoperability faults across enterprise software technologies with execution platform is proposed. A mathematical relationship is established between the control objectives of an information technology and associated technical issues occur in the resources and processes, so that the possible business risks can be minimized within the COBIT framework. The existing acts and regulations for the information technology sectors are applied to bring a ubiquitous model where the customer's issues can be reported through different forms of reliable information services using the established, fault-prone mobile and web technologies. The compliance fault or any non-compliance is considered as the logical combination of the respective processes or entities in that phase and the non-utilization of the resources allocated for that process. The workflow model determines the location of the interoperability faults in case of reliable services and generates the verification report based on the audit and review findings. As per the goal of such business framework encompassing multiple entities and dynamic associations, the different types of risks are identified and reported as a verification chart.

The different types of risks in the IT industries, the frequency of occurrences and the impact also identified and scaled within acceptable limits. The gaps between the possible and realizable objectives are the focus points to minimize the existing regulatory violations and risks by solving the technical issues through proper control strategies. The relationship between the hazard levels in the organization and the impact of those hazards are plotted as results of the work which has been substantiated by a case study on the information services of a web based healthcare or Healthcare management system. The various interoperability faults in the declared web services are in the forms of non-agreements between two essential services, expiry or non-licensing of one service on the deployment platform and non allocation of resources in another service when the interface is enabled for requesting the same resources. The mathematical model produces the way for enhanced implementation of the strategic plans as per the Indian IT business environment.

The very basic limitation of the proposed distributed compliance management model for enhanced governance is the lack of sensitivity and scalability of the model. The model cannot be scaled into IT businesses if the size is beyond that of small and medium enterprises (SME). The sensitivity of the system in terms of the amount of impact of a specific risk with respect to a small change in its control objectives and technical issues will be considered in the future works.

Acknowledgements:
The authors' research work is partially funded by Bharathiar University under the award of University Research Fellowship. The author of this paper would like to sincerely thank Prof. Dr. S. Chandrasekaran (WSEAS Member) for his valuable guidance during the course of this work. The author also would like to thank the unknown reviewers for valuable suggestions that improved the presentation of this paper considerably.

References:

[1] Marwane El Kharbili, Business Process Regulatory Compliance Management Solution Frameworks: A Comparative Evaluation, *8th Asia-Pacific Conference on Conceptual Modeling, Australian Computer Society,* Vol. 130, 2012, pp. 1-10.

[2] Mohammad Hamdaqa, Abdelwahab Hamou-Lhadj, An approach based on citation analysis to support effective handling of regulatory compliance, *Journal of Future Generation Computer Systems, Elsevier Publications*, Vol. 27, 2011, pp. 395–410.

[3] The True Cost of Compliance, *A Benchmark Study of Multinational Organizations, Ponemon Institute,* January 2011, pp. 1-32.

[4] Christopher J. Pavlovski, Joe Zou, Non-functional requirements in business process modeling, *5th Asia-Pacific Conference on Conceptual Modeling(APCCM), Australian Computer Society, Inc.,* Vol. 79, 2008, pp. 103-112.

[5] Huy Tran, Uwe Zdun, Ta'id Holmes, Ernst Oberortner, Emmanuel Mulo, Schahram Dustdar, Compliance in service-oriented architectures: A model-driven and view-based approach, *The Journal of Information and Software Technology, Elsevier Publications,* Vol. 54, 2012, pp. 531-552.

[6] G. Kannabiran, K. Sankaran, Determinants of software quality in offshore development–An empirical study of an Indian vendor, *Journal of Information and Software Technology, Elsevier Publications,* Vol. 53, 2011, pp. 1199–1208.

[7] Kevin Kam Fung Yuen, Henry C.W. Lau, A Fuzzy Group Analytical Hierarchy Process Approach for Software Quality Assurance Management: Fuzzy Logarithmic Least Squares Method, *Journal of Expert Systems with Applications, Elsevier Publications,* Vol. 38, 2011, pp. 10292–10302.

[8] William Mahoney, Robin A. Gandhi, An integrated framework for control system simulation and regulatory compliance monitoring, *International Journal of Critical Infrastructure Protection, Elsevier Publications,* Vol. 4, 2011, pp. 41-53.

[9] Thomas Murphy, Kathryn Cormican, An analysis of non-observance of best practice in a software measurement program, *Proceedings of the 4th International Conference on ENTERprise Information Systems-aligning technology, organizations and people, Journal of Procedia Technology, Elsevier Publications,* Vol. 5, 2012, pp. 50 – 58.

[10] Partha Saha, Ambuj Mahanti, B.B. Chakraborty, Avinash Navlani, Development of Ontology Based Framework for Information Security Standards, *Proceedings of the* 9th *International Conference on Autonomic and Autonomous Systems,* 2013, pp 83-89.

[11] Viljan Mahnic, Natasa Zabkar, Assessing Scrum-based Software Development Process Measurement from COBIT Perspective, *Proceedings of the 12th WSEAS International Conference on Computers,* 2008, pp. 589-594.

[12] Aneesh Zutshi, Antonio Grilo, Ricardo Jardim-Goncalves, The Business Interoperability Quotient Measurement Model, *Journal of Computers in Industry, Elsevier Publications,* Vol. 63, Issue 5, 2012, pp. 389-404.

[13] Guido Governatori, Antonino Rotolo, A Conceptually Rich Model of Business Process Compliance, *Proceedings of the 7th Asia-Pacific Conference on Conceptual Modelling (APCCM),* Vol. 110, 2010, pp. 3-12.

[14] Shazia Sadiq, Guido Governatori, Kioumars Namiri, Modeling Control Objectives for Business Process Compliance, *Proceedings of the 5th International Conference on Business Process Management, Lecture Notes in Computer Science, Springer-Verlag,* Vol. 4714, 2007, pp 149-164.

[15] Jessica Young Schmidt, Annie I. Ant´on and Julia B. Earp, Assessing Identification of Compliance

Requirements from Privacy Policies, *Proceedings of the 5th International Workshop on Requirements Engineering and Law (RELAW)*, 2012, pp. 52-61.

[16] Dimitris Karagiannis, A Business Process-Based Modeling Extension for Regulatory Compliance, In Multikonferenz Wirtschaftsinformatik, Munich, 2008, pp. 1159-1173.

[17] Silvia Ingolfo, Alberto Siena, John Mylopoulos, Angelo Susi, Anna Perini, Arguing regulatory compliance of software requirements, *Journal of Data and Knowledge Engineering, Elsevier Publications*, Vol. 87, 2013, pp 279-296.

[18] Oktay Turetken, Amal Elgammal, Willem-Jan van den Heuvel, Mike Papazoglou, Enforcing Compliance On Business Processes Through The Use Of Patterns, *Proceedings of the 19th European Conference on Information Systems"*, 2011, pp. 1-13.

[19] Filip Caron, Jan Vanthienen, Bart Baesens, Comprehensive rule-based compliance checking and risk management with process mining, *Journal of Decision Support Systems, Elsevier Publications*, Vol. 54, 2013, pp. 1357-1369.

[20] Christian Raspotnig, Andreas Opdahl, Comparing risk identification techniques for safety and security requirements, *The Journal of Systems and Software, Elsevier Publications,* Vol. 86, 2013, pp. 1124-1151.

[21] Gabriela Gheorghe, Fabio Massacci, Stephan Neuhaus, Alexander Pretschner, GoCoMM: A Governance and Compliance Maturity Model, *Proceedings of the 1st ACM Workshop on Information Security Governance*, 2009, pp 33-38.

[22] Guido Governatori, Jorg Hoffmann, Shazia Sadiq, Ingo Weber, Detecting Regulatory Compliance for Business Process Models through Semantic Annotations, *Lecturer Notes in Business Information Processing, Springer Berlin Heidelberg,* Vol. 17, 2008, pp 5-17.

[23] Mirko Montanari, Roy H. Campbell, Attack-resilient Compliance Monitoring for Large Distributed Infrastructure Systems, *Proceedings of the 5th International Conference on Network and System Security (NSS), IEEE,* 2011, pp. 192-199.

[24] Aditya Ghose, George Koliadis, Auditing Business Process Compliance, *Proceedings of the International Conference on Service-Oriented Computing (ICSOC), Lecture Notes in Computing Science,* Vol. 4749, 2007, pp 169-180.

[25] Alexander Davis, Du Zhan, A comparative study of SOAP and DCOM, *The Journal of Systems and Software, Elsevier Publications,* Vol. 76, Issue 2, 2005, pp 157–169.

[26] Jolita Ralyte, Manfred A. Jeusfeld, Per Backlund, Harald Kuhnd, Nicolas Arni-Bloch, A knowledge-based approach to manage information systems interoperability, *Journal of Information Systems, Elsevier Publications,* Vol. 33, Issues 7-8, 2008, pp 754-784.

[27] Steven De Haes, Wim Van Grembergen, Roger S. Debreceny, COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities, *Journal of Information Systems, Spring,* Vol. 27, No. 1, 2013, pp. 307–324.

[28] Nicolas Racz, Edgar Weippl, Andreas Seufert, A process model for integrated IT governance, risk, and compliance management, *Proceedings of the Ninth International Baltic Conference on Databases and Information Systems, University of Latvia Press,* 2010, pp 155-170.

[29] Jianping Li, Minglu Li, Dengshengssss Wu, Hao Song, An integrated risk measurement and optimization model for trustworthy software process management, *The Journal of Information Sciences, Elsevier Publications,* Vol. 191, 2012, pp 47-60.

[30] William R. Bush, Software, regulation, and domain specificity, *The Journal of Information and Software Technology, Elsevier Publications,* Vol. 49, Issue 1, 2007, pp 44-54.

[31] Kanchana Natarajan, Sarala Subramani, "Compliance Management Model for Interoperability Faults towards Governance Enhancement Technology" *Proceedings of the 3rd Computer Science On-line Conference (CSOC 2014),* pp 179-188, 2014.

[32] Viljan Mahnic, Natasa Zabkar, Using COBIT Indicators For Measuring Scrum-Based Software Development, *WSEAS TRANSACTIONS On COMPUTERS*, Issue 10, Vol. 7, October 2008, pp 1605-1617.

[33] Clotilde Rohleder, Quality Control and ISO Quality Compliance in the Product Lifecycle Management at Siemens, *WSEAS TRANSACTIONS On COMPUTERS*, Issue 3, Vol. 8, March 2009, pp 469-481.

[34] Hui-Ling Lin, Shao-Shin Hung, Derchian Tsaih, Chiehyao Chang, Web Service-Driven Framework for Maintaining Global Version Consistency in Distributed Enterprise Portal, *WSEAS TRANSACTIONS on COMPUTERS,* Issue 4, Vol. 8, April 2009, pp 620-630.

[35] Mario Spremic, "Measuring IT Governance Performance: a Research Study on CobiT- Based Regulation Framework Usage", *INTERNATIONAL JOURNAL OF MATHEMATICS AND COMPUTERS IN SIMULATION*, Issue 1, Volume 6, pp 17-25, 2012.