Engineering Perspective on Enterprise Software Quality towards Compliance Management for better GRC

KANCHANA NATARAJAN¹, RAMYACHITRA DURAISAMY²

¹ & ² Department of Computer Science, Bharathiar University, Coimbatore, INDIA

¹kanchananatarajan@live.com, ²jaichitra1@yahoo.co.in

ABSTRACT

Ensuring compliance with certain standards is highly complex as per the defined set of rules and regulations. Software compliance life cycle involves modelling, implementing, auditing and governance. The increasing relia nt of software based high-tech applications has larger impact on compliance in such cases of automotive, avionics, medical, railway, financial, nuclear sectors and so on. In the present scenario, IT industries pay much attention on overwhelming set of development features such as quality, security, maintainability, reusability, reduced development cost, certification etc.; whereas fails to concentrate with safety and security standards of the domain which leads the way to non-compliances. Non-compliances of any software can be eliminated by appropriate tracing of requirements based on certain standards of laws and regulations followed throughout the development of structured secure software. This paper enlightens the perspective study on hindering issues of various non-compliances towards the better enhancement of governance, risk and compliance (GRC) technology. The paper also focused to emphasize the major compliance resources available for the applicable domains towards the enhancement of high-level objectives of applications or services.

Keywords: compliance; governance; non-adherence; standard; risk; management; resources;

1. INTRODUCTION

The Software Engineering Standards Committee (SESC) defined set of standards is considered to be the basis for complying the organizational practices and procedures. Standards are defined as the documented agreements which contain specifications or technical guidelines used to make sure the product or process development robust for the purpose of use. Standards are complex and large thus compliance should be managed rather to inflict. The aspect of compliance can be forecasted on organisational level along with the integrated set of standards rather than the project level [1]. The degree of compliance can be determined by checking of the documents against constraints which are defined as per the standards of the domain [2]. Compliance management is a more difficult and challenging task while engineering large systems like telecommunications, defense and aerospace sectors. The high-level software and systems engineering standards such as ISO 9000, ISO 12207, and IEEE 1074 are usually implemented in industry for several reasons in case to meet out the customer demands, process improvement requirements etc., [3].

1.1 Software Product Quality Standards and its Attributes

According to the standard ISO 8402 the term quality is defined as “the totality of characteristics of an entity that tolerate on its ability to satisfy stated and implied needs.” The recent ISO/IEC 9126 (2001) standard for software product quality evaluation has been revised as ISO/IEC 25010 (2011) is considered as a part of SQuaRE (Software product Quality Requirements and Evaluation) series of standards which is applicable for both software products and computer systems [5, 11]. The ISO/IEC 9126-1 standard [4, 5, 6, 7] defines the structured set of quality attributes which are categorized into 6 high-level characteristics and 27 sub-characteristics to evaluate the quality of any software product which is demonstrated in the quality tree as shown in fig.1.

The six high-level characteristics such as functionality, reliability, usability, efficiency, maintainability and portability have direct impact on the architecture which may affect the internal quality of the software [10]. The term ‘quality’ can be defined as the capability of the software product which satisfies the user’s requirements. The requirements are classified as functional and non-functional requirements based on the structural and behavioural issues, technological constraints and so on. The quality of the software can be determined based on the internal quality, external quality and quality in use. The internal quality influences the external quality and thereby the external quality influences the quality in use. Thus the internal quality, external quality and quality in use are interdependent which can be measured by means of internal measure, external measure and quality in use measure. The internal quality can be evaluated by internal attributes of the software [8, 9]. For example: compliance with design modularity and coding standards. The external quality of the software can be measured during the software execution.

1.2 Governance, Risk and Compliance Management

The concept of Governance, Risk and Compliance (GRC) is a holistic approach to ensure the core business by reducing the risks to manage the internal controls, economic instability and performance. The main goal of GRC discipline is to coordinate information and activities across governance, risk and compliance management in order to create and ensure efficiency, knowledge sharing and reporting. The core disciplines governance, risk and compliance management consists of four basic components such as strategy, processes, technology and
people. Each of the disciplines may impact the same components and also these three disciplines may build the information of assessment to the other two disciplines. Recently the disciplines and its components are combined in an integrated and organization wide approach to achieve the objectives of efficiency and

![Diagram of Software Quality Attributes and Sub-Attributes (ISO/IEC 9126-1)](image)

**Fig. 1. Software Quality Attributes and Sub-Attributes (ISO/IEC 9126-1)** effectiveness [12]. It is very difficult to find a holistic view in an organization due to the increased changes in technologies, market globalization, GRC related requirements, regulations and policies etc., The most important and focused GRC areas are considered to be financial and audit GRC, IT GRC and legal GRC which are intended to ensure the operations of all financial processes, the present and future needs of any IT business mandates and legal compliances of organizations. Gartner stated the broad GRC market which includes the areas of financial and audit GRC, IT GRC management and Enterprise Risk Management [13, 14].

1.3 Enterprise Governance of IT

The governance, risk and compliance (GRC) management is the optimal way for attaining strategic and potential benefits of effective enterprise governance of IT. The global software development processes of organizations have higher impact on ensuring and demonstrating high-level objectives as per the standards of regulations of the particular domain. The integration of enterprise software applications and its services depends on the selection of right architecture or group of architectural styles to mitigate risks [14, 15]. In 1990’s, the concept of software compliance seems to be a non-issue but as of now due to the economic effects it’s a crucial business issue with high cost and regulatory implications. The term ‘software compliance’ means ensuring that the software systems of an organization which act in accordance to the regulations, laws and business policies. The section 2 of the paper focuses to list and discuss the various approaches that exist to handle different non-compliances which are proposed by several authors. The section 3 discusses the various software compliances that are involved with the organizations activities to ensure governance risk and compliance (GRC). The section 4 of the paper highlights the various compliance resources that are applicable for different set of domains. The section 5 and 6 of this paper discusses the importance to ascertaining the compliance cost before the product development life cycle.

2. EXISTING COMPLIANCE VERIFICATION APPROACHES AND ITS ISSUES

In organizations any type of compliance violations will lead to the crisis of serious issues of complexity, productivity, trustworthiness, maintainability, reusability, losses of reputation, and penalties [16]. The compliance verification is a typical task also an efficient way to avoid any violations and non-compliances at the earlier stage. Compliance checking of process models is considered to be a tedious activity which involves compliance requirements are gathered according to the defined specifications. There are many existing approaches that tackles the stakeholder’s requirements but none among them links the explicit gap between technical issues and business risks. Several existing techniques for compliance verification are discussed in this section in order to identify its pros and cons.

A) Pattern Based Approach(or) End-to-End Approach

The end-to-end pattern based holistic approach are designed for the specification of compliance requirements visually by using Business Process Model Notation Query (BPMN-Q) which has major advantages such as defining compliance requirements without the detailed knowledge of formal specification languages and visually constructing patterns [17]. Ahmed Awad et. al presented the end-to-end pattern based approach for specification of compliance requirements and verification by visual language called BPMN-Q. In many cases of verifying compliance on model level is highly complex task while it is much easier to resolve violations at the initial stage proceeding to execution [19].

B) Fuzzy Method

The modified fuzzy Logarithmic Least Squares Method (LLSM) is proposed to evaluate the software quality. The limitations with this approach is not applicable for software applications such as web applications, window
applications, distributed applications, mobile applications, and database applications while the methods or frameworks for direct rating scores of each criteria is quite different [18].

C) Data Envelopment Analysis (DEA) Evaluation

The Data Envelopment Analysis (DEA) evaluation is used for software production measurement which creates best practice group to identify the inefficient units among a set of observed units. DEA is also considered to be a management technique which provides comprehensive analysis of comparative efficiencies in case of multiple-input-multiple-output state. Thus the approach also assesses the range of inefficiencies and improves the possible inefficient units. Several authors used DEA techniques in various facets to estimate the productive scale size and to study and analyze the project characteristics of software maintenance process. This approach is widely used by many banks during Y2K date retrofit compliance to measure the project data [20].

D) Other Approaches

For the past two decades, the business process management has increased a lot of consideration with effect to improvement in structure and analysis, changes of enterprises audits, executing and improving the business underlying processes. Even though there exists two disadvantages i.e the maximum part of solutions are not integrated with the defined solutions and BPM approach correlated with other management approaches like Governance, Risk and Compliance (GRC), Quality Management (QM), Audit Management (AM) and etc., The approach supports only for large scale environments to ensure overall management.

Paul W.H. Chung et. al [21] presents process-level compliance flow management and error identification against standards of IEC61508 for safety and ISO9001 for quality assurance. The limitation with existing approach is the lack of the ability to ensure that the specification and execution of a process are compliant with the standard. Kadriye OZBAS-CAGLAYAN et.al [22] presents an approach of software repository analysis to determine the compliance levels of design and code. The authors study also reveals the several existing approaches such as Object Modeling Technique (OMT), Software Reflexion Model technique, software repository mining technique, vector space model and text mining techniques to extract and analyze compliance levels of design and code efficiently.

Panuchart Bunyakiati et. al [23] proposed Java UML Lightweight Enumerator (JULE) tool to diagnose the non-compliance issues and enumerate a set of test cases for extensively testing modeling tool. The tool focuses on model analysis of software modeling tools used to assess the compliance of an open source software tool - ArgoUML. Roy Oberhauser [24] demonstrated an approach which enables the capability of automatic test detection by using the SEEEEK (Software Engineering Environment Event-driven framework) to support adaptable processes for ensuring process compliance and supporting governance. The SeeEEK approach addresses the compliance and governance of software engineering processes for process maturity and effectiveness.

3. THE DIVERSITY OF SOFTWARE COMPLIANCES

Software compliance is considered to be a multidimensional aspect applicable with any type of business process management (BPM) activities in the organizations. The Governance, Risk and Compliance (GRC) management of enterprise IT involves diverse categories of software compliances which are discussed below in detail.

a) Regulatory Compliance (RC)

The whole thing in the software universe revolves around regulation. Regulatory compliance is considered to be one of the most wide spread problem in the area of business process management. Regulatory compliance (RC) is nothing but the act of management for ensuring that the resources of software or services (people, technology, data, application) are structured and act in accordance with the guidelines specified as per the pre-defined regulations (e.g., COBIT standard for IT business framework) [25]. The current raise on consideration towards regulatory compliance involves a number of facts such as corporate scandals, business assurance, trade barriers, and protection of sensitive secure information.

b) Statutory/Legal Compliance (S/LC)

Statutory Compliance (SC) or Legal Compliance (LC) is the procedure to ensure whether the entire software development process of the industry adheres to certain laws, regulations and business polices. Laws and regulations change very frequently by improving the old legislation or by defining new legislature. To develop more secured software, the security requirements have to be observed from the earlier stages of the development process along with its environment [26].

c) Standard Compliance (SC)

Standard Compliance (SC) can be ensured by adopting the particular standards of the domain. It generally defines best practices for the development of certain secure software development process which are represented in the form of documents and guidelines. Many existing and recent standards are available to make sure the safety and security of software such as ISO 26262, IEC 61508, DO-178B and BS 7925 [27].

d) Process Compliance (PC)
Process Compliance (PC) can be carried out in the process level by corresponding objects and their relationships. The compliance objects such as standards, laws, regulations or polices whereas the relationships may be technical, managerial or legal in the process level. The process compliance is the efficient way to detect faults in the software development process. [28].

e) Policy Compliance (PoC)
Policy Compliance (PC) is one of the major global corporate issues which can reduce the risk of internal and external threats in order to improve the efficiency, increased productivity and quality of software services. Policy Compliance is a document which instructs the internal activities of processes that adhere accordingly to follow. The policy elements can be managed by the risks, entities and controls associated with the policy. The IT policy compliance is a complete set of framework which includes standards and procedures, technology controls, high-level policies, business awareness and training, risk assessments, internal and external auditing [29].

f) People Compliance (PeC)
One among the main component of GRC is considered to be people may introduce great amount of uncertainty or flaws in software compliance program. Compliance violations arise due to the errors or exception made by people which may be accidental or purposeful [30].

g) Procedural Compliance (PrC)
Procedural Compliance (PrC) is an adherence of right procedures for obtaining consistency and integrity with the outcomes of task completion. It is an integral aspect of the operational safety of the software system considered to be a highly critical issue which affects the quality of the software product. It can be measured with the help of negative reports submitted by regulators, internal audit and assessors [30].

4. COMPLIANCE RESOURCES WITH DIFFERENT DOMAINS
The software compliance resources usually instruct to follow the best business practices to ensure and sustain the high-level objectives such as quality, privacy, trust, security, licensing, certification and risk management. It is very difficult to formulate a model that able to accommodate all the compliance sources in the software systems of an organization. In the present practice, the compliance issues are implemented on a per-case basis by using hard-coded, ad-hoc solutions which are repulsive because they are hard to change, maintain, reuse, and understand. And also it is difficult to ensure with constant changes in standards, regulations, laws and policies. Some of the diverse compliance sources of applicable different domains are Control Objectives for Information Technology (COBIT) [15, 24, 27, 32,33], Health Insurance Portability and Accountability Act (HIPAA) [15, 33], Payment Card Industry Data Security Standards (PCI DSS), Sarbanes-Oxley Act (SOX) [15], Federal Information Security Management Act (FISMA), Foreign Account Tax Compliance Act (Facta), Information Systems Audit and Control Association (ISACA), Markets in Financial Instruments Directive (MiFID), French Financial Security Law (LSF), Basel II Accord, International Financial Reporting Standards (IFRS), and Tabaksblat [30, 31, 32]. The various information security and asset management ISO standards include ISO/IEC 27002:2005 (Code of Practice for Information Security Management), ISO/IEC 27001:2005 (Information Security Management System - Requirements), ISO/IEC 15408 (Evaluation Criteria for IT Security), ISO/IEC 13335 (IT Security Management) and ITIL (OR ISO/IEC 20000 SERIES) [32].

A. Control Objectives for Information and Related Technology (COBIT)
COBIT is an IT framework which contains set of guidelines for IT governance that helps the organizations to develop control structure to bridge the gap between IT objectives, technical issues and business requirements. COBIT 5 combines COBIT4.1, Val IT and Risk IT into a single framework that acts as an enterprise framework and operable with TOGAF and ITIL. It consists of mainly four control structures such as a) Planning and Organization, b) Acquire and Implementation, c) Deliver and Support, d) Monitoring. The COBIT components include Framework, Process descriptions, Control objectives, Management guidelines, Maturity models. COBIT security focuses on particular risks around IT security in a mode that is simple to track and execute for small and large organizations [32].

B. Health Insurance Portability and Accountability Act (HIPAA)
The Health Insurance Portability and Accountability Act (HIPAA) also known as public law 104-191 was enacted in the year 1996 as part of the healthcare reform during President Clinton’s second term to ensure security, privacy and portability of medical insurance and health information [32]. HIPAA comprised with set of rules and supports the most important features such as accessibility and portability, group provisioning and revenue, privacy, security, and taxation which cover the standardization of the healthcare delivery process to be efficient. The lacking with access control model to enforce HIPAA rules is one mandatory issue. The most common issue that affects HIPAA modeling is the legal document structure, complexity of legal document language, cross-references and exceptions. Thus the rules are defined to ensure the privacy of patient details. Particularly, HIPAA title II addresses five security and privacy rules that must be financed by healthcare institutions to protect patient electronic records against attacks and fraudulent use.
C. Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS involves information security policies and procedures for the protection of credit card sensitive data. Standards are defined to secure information against abuse or other electronic risks. PCIDSS specifies six major objectives; first, transactions should be conducted through secured network to ensure firewalls are robust which determines the vendors / cardholders convenience. Secondly, cardholder information must be protected wherever it is stored. When cardholder information are transmitted through public networks then the data must be encrypted. Third, system should be protected against the activities of malicious hackers by frequently updated anti-virus software; malware solutions to make sure all applications are free of bugs. Fourth, access to system information and operations should be restricted and controlled. Fifth, network should be constantly monitored and regularly tested to ensure that all security measures and processed are in place and functioning properly. Sixth, a formal information security policy must be maintained and followed at all times and by all participating entities [31, 32].

D. Sarbanes-Oxley Act (SOX)

The Sarbanes–Oxley Act (SOX), which is also known as the Public Company Accounting Reform and Investor Protection Act, was enacted in July 2002. SOX have been introduced after series of corporate scandals due to false reporting of financial and accounting statements. SOX require every organization to have their control framework to monitor the processes for financial reporting. For auditors, to access the adherence to SOX requirements, they have to understand the framework used by the organization that helps to understand the access control of applications used to ensure authenticity, security and integrity of the information flow between systems, confidentiality of electronic records etc. The collected information from the report can be seen as requirements for information security programs which help in security assessment [32].

E. FISMA & FIPS

FISMA stands for Federal Information Security Management Act is a branch of the US E-Government Act (Public Law 107-347). It needs US federal agencies to develop, document, and implement to provide information security that support the operations and assets of the agency. FISMA includes Periodic risk assessments of information, Periodic evaluation and testing, Security awareness training, Risk-based policies and procedures. The Federal Information Processing Standards (FIPS) publication series of the National Institute of Standards and Technology (NIST) is an official series of publications relating to standards and guidelines adopted and made available under the provisions of the FISMA30 [32].

5. COST OF SOFTWARE COMPLIANCE AND NON-COMPLIANCE

A benchmark study conducted by Ponemon Institute and Tripwire Inc on 46 multinational organizations of all industries shows the research report which states that, “The cost of non-compliance can be more expensive than investing in compliance activities”. In case of IT industry the study defines that the cost of non-compliances 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 [33].

Fig. 2. Compliance Cost and Non-Compliance Cost of IT Industry

6. SOFTWARE COMPLIANCE IS VITAL. WHY?

The worldwide loss of hundred billion dollars in Y2K (2000) issue is due to the reason of non-compliances. The Y2K ‘bug’ was challenge without any guide to guarantee by means of programmers efficiency in maintaining code, production process and performance. Corporate banks by yearly spend hundreds of millions of dollars in software though the issue is extensive in fact [20]. In the year 2003, Garner group estimated that the worldwide expenditure on software by users exceeds $730 billion and packaged software market rated as $176 billion. Even the stakeholder’s are not satisfied with the quality of the software. Hence the stakeholder’s purpose of use includes decision making process, audit and monitoring contracts, reporting etc., Thus software ‘bug’ is an error, fault or failure in software program may arise due to the reason of improper source code design or
framework as per the guidelines specified. For ensuring software compliance, it is estimated that $17.6 billion spent for health care domain alone over a number of years to align the systematic procedures as per the Health Insurance Portability and Accountability Act (HIPAA) of 1995. In case of business domain to ensure compliance, it is estimated that in the year of 2005, organizations spent $5.8 billion as per the procedures of Sarbanes-Oxley Act (SOX) [26].

7. CONCLUSION
Software compliance will be neither uncomplicated nor easy. Large scale business firms evolve with products to the end users in order to avoid non-compliance penalties, client satisfaction, asset management processes, audit control and report. For example: the products of large corporations for business control and audits are IBM Lotus workplace, SAP GRC Solution, Microsoft Office Solutions Accelerator for Sarbanes-Oxley and so on. Many vendors are actively addressing the compliance issues and currently providing compliance solutions or services meantime the majority of vendors believe that IT compliance is always highly complex without insufficient use of compliance monitoring tools.

REFERENCES
33. The True Cost of Compliance, Benchmark Study of Multinational Organizations, Ponemon Institute, pp 1-31, January 2011.