An Aspect Oriented Process Based Approach To Information Risk Management

Dhanya Pramod[1], R. Raman[2], S. Vijayakumar Bharathi [3]
[1] Professor [2] Professor & Director [3] Associate Professor
Symbiosis International University, Symbiosis Centre for Information Technology, Pune India
[1] dhanya@scit.edu
[2] director@scit.edu
[3] svkbharathi@scit.edu

***Abstract*--In this era of fast paced technological advancements, security issues and risks related to it have become a key concern for all organizations. Enterprise Governance, Risk management and Compliance (GRC) is the popular approach to handle enterprise risks and reduce its impact. This paper focuses on the risk management, especially the risk assessment approaches and proposes an aspect oriented approach to risk management. In this approach, the risk management processes are designed separately from the core business processes and are weaved to the flow of business process steps wherever necessary. This brings the advantage of separation of concerns of risk management from the business process. The design of business processes then need not look into the design of risk assessment related to it. This will enable handling of risk and its assessment by expert risk advisories, those who are specialized in it.**

Keywords: Information Risk Management, Governance, Risk and Compliance, Security, Aspect oriented approach

I. INTRODUCTION

Effective risk management process is an inevitable part of an organizations IT security strategy. It has an impact in the organization's ability to perform their mission. Information risk management frameworks like COBIT and NIST 800-30 are available with guidelines for conducting the risk assessment and mitigation.

Every application or business process may have some non functional requirements in addition to the functional requirements. Aspect Oriented Modeling deals with weaving the non functional aspects to the basic model and thus increases modularity. It complements the Model Driven architecture and helps separation of concerns. Basic functionality and aspects can be designed separately and programmer need not know about the aspects. Whenever the insertion of aspect is required, the same is marked using pointcut in the base model. The collections of these points cuts (join points) are weaved with the additional behavior called aspect advice. The application of this approach is to model cross-cutting issues that occur in various designs as a separate fragment and apply it to existing and newly designed applications. Risk management deals with IT security in an organization. IT security strategy is a cross cutting strategy for business, as it has to intervene at various points of any business. Hence we have adopted an aspect oriented approach for risk management. The proposed model of risk management separates the cross cutting concern from the business process design and modeling. The hot spots in the business processes where the risks may occur will be identified and mitigation methods will be suggested for reducing or avoiding the risk and its impact. In the business process flow when the hotspots are identified, the relevant risk management aspect is weaved in order to integrate the same. The work will study the feasibility and effectiveness of the approach and propose an aspect oriented model for information risk management.

II. LITERATURE REVIEW

The concept of Governance, Risk management and Compliance (GRC) is becoming popular in the organizations and is used for statutory compliance and good governance. GRC provides a convergence platform and controls all the domains in the organization. It facilitates collection, analysis and documentation of risk. The GRC implementation approaches vary[6]. He claims that the process based approach to GRC implementation is more suitable for an organization than other approaches like checklist-based, asset-based and incident-based approaches.

Recently enterprise risk management has drawn attention of organizations world- wide. Risk Scenario analysis is a technique to make IT risk more concrete and tangible and enables proper risk analysis and assessment[7]. It is difficult to identify relevant risks and use of risk scenarios will help to ease the task. There are various approaches to derive risk scenarios and the commonly used approaches are top-down and bottom-up approaches. The most useful way of doing it is by following the sequence given below

Identify Generic scenario, Define concrete scenario, Do validation against business objectives, Refine scenarios, Categorize them according to criticality, Reduce scenarios, Prepare risk list- which have to be followed in the mentioned order

Risk factors influence business and classified as environmental and capabilities. Environmental factors can be external or internal risk factors depending on the control of organization (inside or outside the control of organization). Capabilities are used to assess an organization's efficiency in certain IT related activities. The Information Systems Audit and Control Association (ISACA) frameworks are available and basically used for assessing IT risk management capabilities, IT capabilities and IT related business capabilities. In Risk analysis, frequency and impact of scenarios are assessed based on risk factors and either of the risk response options (avoid, reduce/mitigate, share/transfer, accept) is chosen according to the risk tolerance level. Accordingly the risks are prioritized and handled by developing an action plan.There are many standards, acts and policies that have evolved in the recent years to highlight the importance of security and risk management. Most of the companies still struggle to understand the scope and approach of Sarbanes-Oxley **(**SOX) IT General Controls (ITGC) [1]. It is essential to understand the focus of risk assessment, with specific reference to Confidentiality, Integrity or Availability prior to going ahead with risk assessment.By focusing on the parameters that are critical from the Sarbanes-Oxley ITGC perspective, organizations can save a lot of time, effort and money and also reduce the load on the IT department during risk assessment. The right way to conduct a risk assessment within the scope can be achieved by focusing on risks that are associated with each general control process area, such as change management, logical access, computer operations, job scheduling and third parties/service organizations that manage applications or data centers. SOX focus on data integrity and misstatements to financial reporting by identifying the following risk criteria

Integrity risk: The integrity of application has the impact of parameters like number of changes, number of application controls, developed in-house or otherwise and number of developers.

Access risk: The access to the financial application has the impact of the parameters like number of users, number of administrators, direct access to the underlying database and integrated/independent authentication.

Dan Wilhems[2], emphasizes on the benefits GRC solutions bring to SMEs and describes how they minimize risks, tightens business processes, improves change management, helps drive innovation, increases agility, reduces cost, repetitive tasks in the enterprise resource planning landscape, which can be implemented in stages.John P. Pironti [4], stated that ISRM(Information Security and Risk Management) programs have the strategic advantage in business activities. The alignment of ISRM capabilities with business requirements and activities is vital to the organization mission. When evaluating the ISRM programs and its capabilities it is mandatory to look into the key factors like comprehension and acknowledgement of current business conditions, Governance models that will be utilized, Alignment with the organizational risk profile, Metrics and measures. It is also essential to consider budget and sourcing plans and communication and awareness plans.The currently available literature throws light only on a process based approach to GRC. This does not adequately cover on ease of designing risk management procedures and its integration into business process. All the above methods needs the people who are involved in business process to know the risk management. Hence we felt the need for an aspect oriented perspective to risk management, wherein design of risk management aspects is separated from business process design. Aspect Oriented Approach has been used for handling security issues of applications and proved to be good. Dhanya Pramod [3] states that aspect oriented approach can be used for integrating security attack countermeasures into web based applications without changing the core application.

III.ASPECT ORIENTED APPROACH TO GRC

The fundamental elements of Aspect Oriented Modeling (AOM) are aspect, advice, point cut and joint point[5]. Aspect is a nonfunctional concern that is scattered across multiple modules or classes of a system and is put together with other functional concerns. Joint point is a well defined point in the structure or execution of a system and can be called as a static joint point and dynamic joint point respectively. Pointcut is the collection of joint point. Advice is the behavior that is injected by the aspect to the joint points. The best feature of AOM is the injection of advices before, after and around joint points. This is accomplished by a process called weaving.

In this section we have proposed how aspect oriented approach can be applied in risk assessment approaches. In Checklist based approach auditors make a checklist and compare the implementations against it for testing requirements. This approach can be converted into an aspect oriented approach. Preparation of checklist will be an aspect. As there are different areas to be covered in the checklist, for each of them separate checklist can be made through different aspects and later on these aspects can be chained to link the area-wise checklist. For comparing the implementation against checklist, aspects can be created area-wise. This checklist based method is simple but lacks rigor. The reason being the checklist by default lacks comprehensiveness and accuracy.

In Asset based method Information assets are identified and then the associated vulnerabilities and threats are identified. Accordingly risk impacts are calculated and mitigation measures are suggested eg: OCTAVE, ISO 27001.To incorporate aspect oriented concepts in asset based method following steps are used.

A. Define Asset identification aspect: In this step all information assets are identified.

B. Identify specific aspects:

B1. Identify and define vulnerability identification aspects

B2. Identify and define threat identification aspects.

C. Calculate the risks: In this step, in order to calculate risk, a specific aspect is defined

D. Mitigation: this step is to propose and define mitigation method as an aspect . This method is rigorous and comprehensive. It is not a proactive approach.

The Incident based approach is based on the past incident reports. The first step is to gather incident details from earlier reports, then investigate incident to gather past deviations. Separate aspects are defined to gather incident, investigate and then recommend mitigation methods. The advantage in this method is, it gives an indication about the level of exposure and allows organization to deal with it by reviewing the business processes. The flip side of this approach is, if the impact of incident is high then mitigation is not possible. A Process-based approach is built on the fact that exploitation of vulnerability in the process cause risks. In this approach, all the causes have to be analyzed before plugging the vulnerabilities. This would help in solving the problem in an efficient manner. In this approach there is a need for business process analysis. The vulnerabilities in the process and the interface between processes have to be identified. A hierarchical view of processes in the organization is created to understand the details and relationship between each process. Every process is analyzed in detail to find out roles, Entities, Application programs, Data-tables, Documents-input/output and Controls. During the audit process auditor should select few processes for auditing based on criticality, financial implication, outsider interaction, customer interaction, change status etc. Aspect oriented approach to this method defines aspects for the following: Identify process aspect, select sample process, find role, find entities, find application programs, find data-tables, find I/O documents, find risks and find controls, verify process and inject control and risk mitigation. We propose an aspect oriented process based approach for risk Management.

To illustrate the proposed method, the process for opening a savings bank account is being considered. The diagram (fig 1) depicts steps of the basic functionality. The various risks that are identified in the process are incorrect application, incorrect information and inconsistent information. During “verify prospective depositors” the possible risks are invalid identity, invalid address, invalid job details, invalid income details and invalid asset details. During KYC the risks involved is for example invalid Permanent Account Number (PAN).

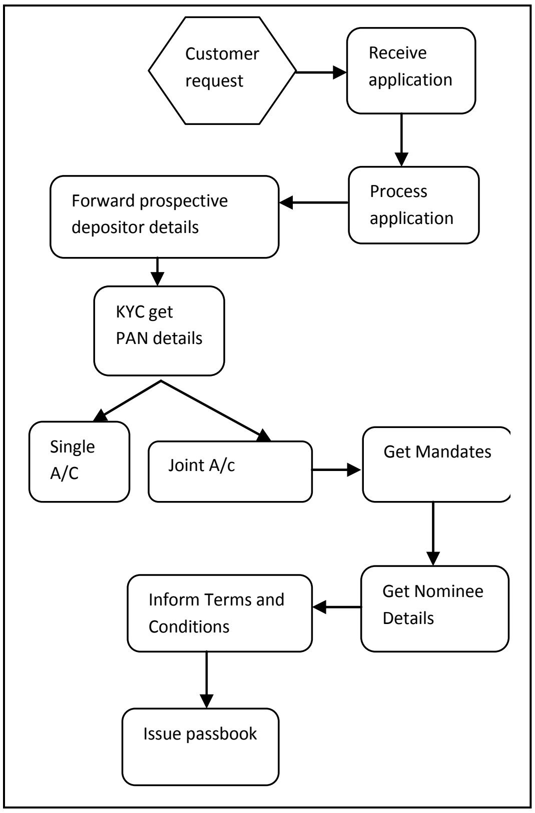

Fig. 1. Process for creating an account in the bank.

To incorporate risk management into the said scenario, aspect oriented approach is recommended as follows.

Verify Application aspect is defined to take care of the risks inherent in the received application. The hotspot for injecting this aspect would be “process application” pointcut. Verify depositor Details aspect is defined to check the accuracy of information provided by the user and injection pointcut is “forward prospective depositor details”. The bank may collect the PAN details of depositor for KYC policy and risk involved here is handled by checkPAN aspect. An aspect can be injected either before or after or even around the pointcut. The above suggested aspects can be injected “before advices” to check and handle risk. At every pointcut we check for a risk and if we find a risk we call the advice, which defines how the risk to be handled. For example while verifying customer details if the address field is incomplete then the process should be initiated to reject the application. VerifyApplication aspect checks for completeness, correctness and consistency of application information and stop further processing of application if the conditions are not met. Fig(2) depicts the weaving of aspects in to the core business process flow wherein two sample aspects are shown.

New aspects can be defined and integrated into the core business process anytime. For example if submission of Unique Identity Number (UID) or Social Security Number (SSN) proof is added as a requirement, then we can have a new aspect for verifying the details related to it and then handle the noncompliance as defined.

IV.RESULTS AND DISCUSSIONS

We propose a model Fig.3 for process based risk assessment which is based on the aspect oriented approach. The elements of model are

- Core business process flow
- Risk assessment aspects
- Hotspots(pointcuts) in business process flow wherein to inject the risk assessment aspect
- Risk response advice which deals with how to handle the identified risk.

The model presents a modularized approach to problem solving and facilitates easy integration and disintegration of modules. The risks that need to be assessed can be categorized and modeled as a chain of checkpoints that need to be integrated at various hotspots of the business process flow. Whenever the hotspot in the business process flow is reached risk assessment aspect is called and accordingly appropriate risk response advice is executed.

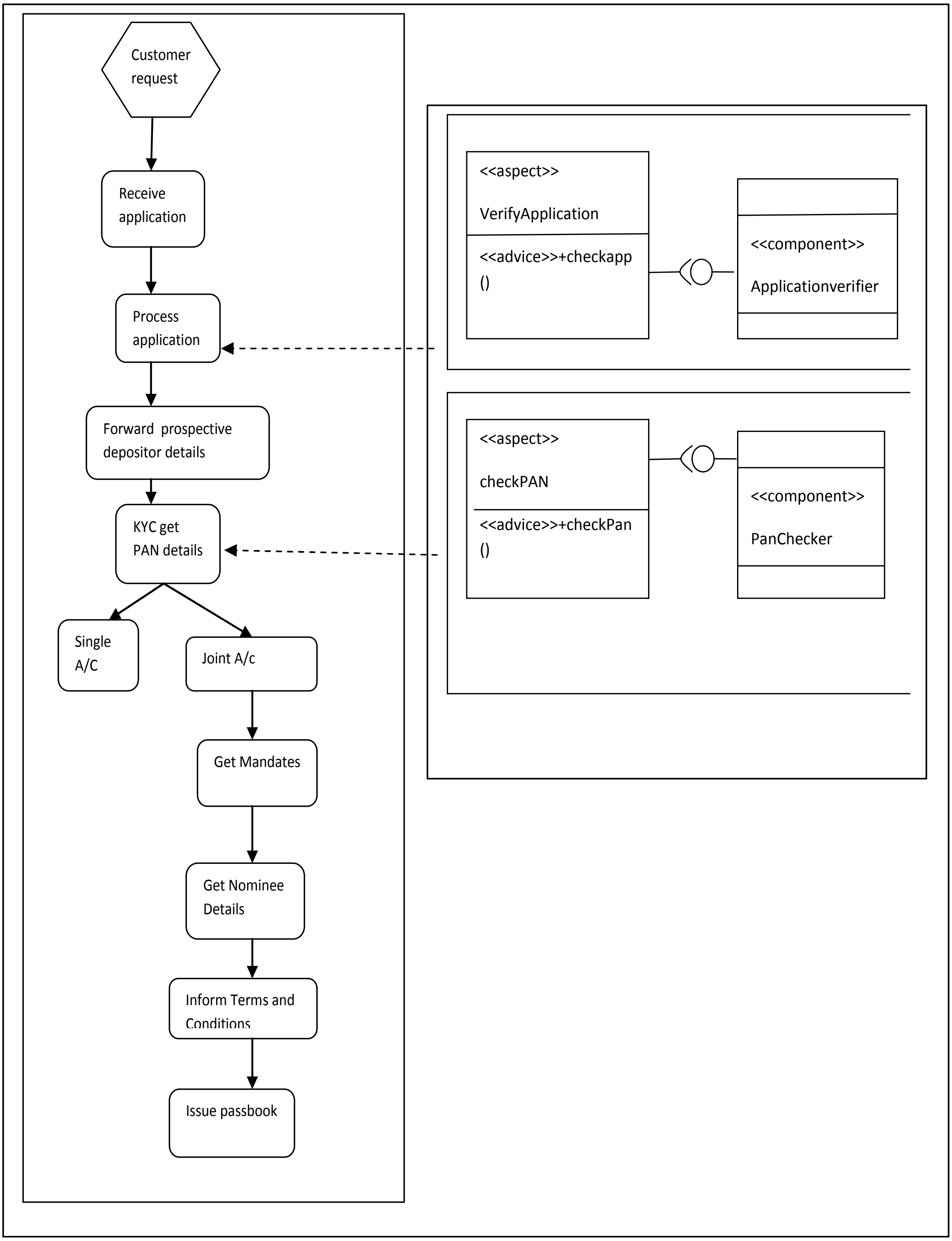

Fig. 2. Weaving of aspects

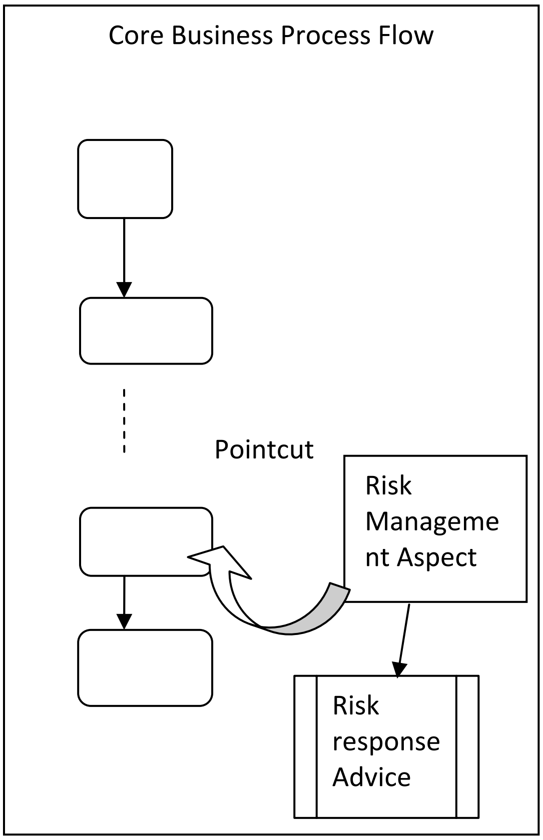

Fig. 3 Aspect oriented Process based model

V. CONCLUSION

Risk Management is an inevitable cross cutting concern for any business. Though frameworks and methods are available for risk management, most of them are asset based or checklist based. The proposed aspect oriented process based approach to risk management not only increases modularity, but helps in incorporating any new assessment aspects that may crop in future. The method ease the risk assessment by allowing separation of risk assessment activity from business process flow, but still weave it in the appropriate steps of business process to maintain the assessment aligned with the core functionality. The future work will focus on how to use commonly used risk assessment frameworks in an aspect oriented approach.

REFERENCES

[1] Arvind Mehta, An approach toward Sarbanes-oxley ITGC Risk assessment, ISACA Journal volume 5, 2010, pp 15-18

[2] Dan Wilhelms, Seven ways SMEs can benefit from GRC solutions,ISACA journal volume 5 2010,pp 20-21

[3] Dhanya Pramod, Vinay Vaidya “A Platform specific UML model for Web Application self Defense through an Aspect Oriented Approach”, International Journal of Computer and Electrical Engineering , Vol. 1, No. 4, October, 2009, 1793-8163

[4] John P. Pironti, key considerations when evaluating ISRM programs and capabilities,ISACA journal volume 1,2011, pp 21-26

[5] S. Clarke and E. Baniassad. Aspect-Oriented Analysis and Design: The ThemeApproach. Addison-Wesley Professional, April 2005.

[6] S .Ramanathan, A case for a process based approach to GRC, ISACA Journal volume 5, 2010 pp 22-26

[7] Urs Fischer, IT Scenario analysis in enterprise risk management, ISACA journal, volume 2, 2011