ISSN NO. 2320-5407

Journal homepage:http://www.journalijar.com
Journal DOI:10.21474/IJAR01

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

Original Internal Control Framework for ERP systems in accordance with SOx 404 compliance and XBRL.

Anubhav Nagpal.
Symbiosis Center for Information Technology, Pune.

Manuscript Info

Manuscript History:

Received: 12 May 2016
Final Accepted: 19 June 2016
Published Online: July 2016

Key words:
SOx/SOA (Sarbanes-Oxley Act), Internal Controls,ERP (Enterprise Resource Planning), Continuous Auditing, xbrl (eXtensive Business Reporting Language), SOD (Segregation Of Duties).

Corresponding Author

Anubhav Nagpal.

Abstract

The paper considers key IT controls in three important business processes in Enterprise Resource Planning (ERP) systems i.e.in Procure-to-Pay, Order-To-Cash and Financial Reporting cycle and proposes an effective internal control framework over efficient financial reportingusing XBRL and hence according to Sox 404 compliance. The paper uses COBITframework as a reference point to identify the IT controls in the systems. Key controls have been further subdivided into application, access and general controls. The paper, with examples, from SAP and Oracle ERP lists out assessment of internal controls, preparing Risk Control matrix and Segregation Of Duties conflict matrix in all the three cycles mentioned above which helps identifying deficiencies and material misstatements. The paper provides a SOx 404 compliant preliminary framework of crucial internal controls for auditors to consider while inspecting Enterprise Resource Planning Systems.

Introduction:-

After the occurrence of numerous worldwide financial scandals, such as Enron, WorldCom, Tyco, Sunbeam the importance of internal control on financial reporting and information security has vastly increased. Losses that a company incurs due to Information security breach are immense. Generally, an attack on information causes theft of confidential data, financial fraud, an incapacitated web server, and corrupted operation data (Gordon et al., 2005). All of such attacks affect the accuracy and reliability of financial data derived from the information system (Walters, 2007). Hence, understanding related risk management and control is critical to any organization implementing the ERP system. Therefore for a better financial reporting mechanism in ERP systems, a well-designed and an effective internal control framework would have an important hand to play. The aim of a firm should be to generate financial reports that are free from material errors, offers better disclosures and mitigates the risk of internal fraud and other activities that make their organization asset deficit and lower their profitability.During ERP implementations in an organization, internal controls and regulatory compliance are the necessary evils of ERP success. Hence, processes shall be designed in such a way that meets regulatory compliance, systems are to be configured to support those processes, and most importantly people need to be trained to execute on these compliant processes. Not to forget, CIOs and CFOs need to institute a framework to ensure that the implemented ERP solution meets SOX and other regulatory requirements after go live and also on an ongoing basis

Why SOx?

Year 2000 to 2002 saw several large corporate companies getting caught in series of frauds especially in area of financial practices and reporting and serious issues like Enron and WorldCom lead to creation of Sarbanes Oxley Law, also called as SOx and known as 'Public Company Accounting Reform and Investor Protection Act. Section 404 of the SOx Act is Assessment of Internal Controls and it states that company must provide a description of its internal controls in attempt to increase confidence of general public as well as investors while allowing them to gain an insight into company's procedures. Also as per section 404, company is required to hire an independent accounting firm to come and audit the accuracy of financial reports.This paper lays much emphasis on IT controls as Information Technology (IT) are critical for achieving SOx compliance cost-effectively.Also, to achieve SOx an

organization shall start as early as possible i.e. enterprise wide initiative should be established with a strong tone at the top with clearly defined roles and responsibilities. We have followed the industrial approach to develop SOx compliant Internal Control framework for ERP systems and the research objectives of this paper are as follows: (1) identifying critical applications relevant to SOA compliance, testing the controls and mitigating the risks forms the basis of this approach, the framework thus selected is COBIT; and (2) how XBRL can help to achieve SOX 404 compliance in ERP systems. This approach puts greater emphasis on the automation of the monitoring of financial processes and control activities, eliminating the scope of manual or semi-automated tests and enabling a complete and accurate view of the control environment and a higher level of confidence. Using Murthy and Groomer continuous auditing web services (CAWS) model for XML-based accounting systems, our approach too proposes IT frameworks for continuous auditing such as extensive Business Reporting language (XBRL) to address the mandates for SOx. It not only reduces the time and costs of the auditing process but can also help a firm to prevent compliance issues before they arise. The internal framework thus developed also addresses the controls that a firm and an external auditor shall consider when XBRL Taxonomy is included.

Step 1- Selecting the framework:-
The starting point for any firm to comply with section 404 shall be identifying the framework that provides a well-defined basis for establishing effective internal controls over financial reporting. Although COSO is the most established control framework for enterprise governance and risk management but it lacks many IT-related controls whereas COBIT on the other hand not only covers IT controls in detail but also adhere to COSO framework i.e. a clear mapping exists between COBIT IT controls and COSO policies and henceforth is recommended.

Step 2- Identifying key Controls in ERP systems with respect to SOx 404 compliance?
Application controls are defined as Programmedand related manual procedures in application software that are designed to help ensure the completeness and accuracy of information processing. According to this approach we list the controls in three cycles as key controls for whole of the ERP system. Following are the primary areas of key controls according to Section 404 compliance:

1. Automated process controls:Automated process controls are codified controls enforced by an application based on programmed code. These controls are developed and maintained by application developers or programmers. For example, In ERP systems, applications are designed in such a way that an unbalanced journal entry will not be allowed to be posted.
2. Manual process controls: It isimportant for an organization to employ critical manual controls because it makes sure the integrity of the data and reliability of financial reporting is maintained. Account reconciliations and approvals are two important examples of manual controls.
3. Interface/integration controls:An SOA compliance approach should be followed to make sure that integration between different applications is considered as risk factors in the financial reporting process. For example, a firm using a payroll application that interfaces with the core financial reporting application should identify and evaluate the controls that would be necessary to counter the inherent risks relating to the "hand-off" of critical data between the two applications.
4. Reporting controls:Reporting controls not only ensure reports generated from the application but also reflect the financial position of the organization. This approach suggests using XBRL reporting for generating efficient financial reports but the compliance team should make sure that all the possible risk from the financial reports are addressed within and outside because if financial reporting controls are not implemented correctly, all of the configurable, application and interface controls are rendered useless.
5. Application security Controls: Segregation of duties (SoD) and Access Controls: This control states that access defined for each role should be free of any conflicting duties i.e. roles shall be allocated to individuals who perform the specific roles defined to ensure that no individual is assigned a combination of incompatible roles that createa conflict or unauthorized access. For e.g., set up a vendor/pay a vendor. It may also result in inappropriate accessto sensitive transactions for e.g., vendor pay data or ability to modify critical application configurations.
6. General computing controls (GCC):General control is one of the critical aspects of key controls. These controls are pervasive across all or most controls and applications. They address the risks that impact the application, including unauthorized changes, access to the application, related database and network, security administration and computer operations

Step 3- Prioritizing Applications:-
One of the most critical partsof the compliance team is to identify and prioritize the applications that are utilized in the high-priority processes and are likely to impact the financial reporting elements. Factors to consider when prioritizing applications include:
• The volume of transactions processed: Higher the volume of transactions processed, the more critical is the application
• Amount of money involved with the transactions: Larger the amount involved more critical will be the application.
• The sensitivity of the data and transactions: the more sensitive data involved, the more critical the application

Step 4-Reviewing "key" controls with Auditor:-
After the applications have been prioritized and controls have been identified by the firm, it is very important to review the list with external auditor so as to identify what all controls to keep in the list because every selected key control shall be tested, documented and remediated and shall be re-tested if found ineffective which is a costly affair. Our approach lists few of the key application and access controls identified in the three crucial cycles of ERP citing examples from SAP and Oracle ERP that the firm and an external auditor shall consider for making the framework SOx compliant.

Application control considerations for the Order-to-Cash (OTC) cycle:-
The Order to Cash cycle in an ERP system includes activities related to the sale, delivery and billing of materials and services to the organization's customers. Throughout this process are various application/configurable controls that shall be considered. Some of them are explained below.

1. Tolerance limit settings: For example, a control that shall allow payment by cash only if the amount is within a certain tolerance limit in relation to the stated invoice amount is in place or not
2. Maintenance of Customer Master Record: SAP provides configurable controls that notify userwith a warning or error/exception message that a possible duplicate record exists based on defined search criteria. This control must be "turned on" to deploy the search criteria. These controls are detective in nature and area report that reviews customer data for duplicates by listing all customers.
3. Inherent control shall include data flow of sales transactions in an organization rely upon the inherent programmed control that this data transfer in the sales cycles occurs accurately and timely.
4. Accurate Billing, Invoicing and Payment Processing: By establishing proper security controls in place, risks of invalid or untimely changes to accounts can be mitigated. One of such important control in Oracle applications or SAP environment is:

Flexfield Value" Security:A flexfield is a set of data segments that an organization can customize according to its business needs without programming. The Accounting Flexfield, for example, helps to identify a unique chart of accounts. Flexfield value security allows an organization to restrict the set of key flexfield segment values that an employee can have during data entry. This control is based the access rules an organization defines.

Cross-Validating Segmentsin Key Flexfields: This configurable control restricts invalid account codecombinations from being created during journal entry processing i.e. it perform an automatic cross-validation of segment values according to pre-defines rules of an organization. This control helps your application to check if it is a valid combination of values before updating the database. If an invalid combination is entered, a message window appears asking you to choose a combination that is already defined.

Application control considerations for the Procure to Pay (PTP) cycle:-
The Procure to Pay process in an ERP includes all activities related to the requisition, order, receipt and payment for materials and services from the organization's vendors and suppliers.

Some of the key PTP controls in an ERP system are:

1. Purchase Order, Goods Receipt and Invoice Matching:In ERP systems, the matching process is a part of the validations occurring prior to the payment of an invoice. The types of options available include:
2. 2-Way – Purchase Order and Invoice match within the tolerances defined by the organization
3. 3-Way – Purchase Order, Receiver and Invoice match within the pre-defined tolerances.
4. 4-Way – Purchase Order, Receiver, Inspection and Invoice documents match according to the tolerances set by the organization. However, an organization can configure its software to set tolerance amounts that are used by

the organization to set acceptable variance limits i.e. differences between 1) a purchase requisition and purchase order, 2) a purchase order and a goods receipt.

Goods Receipt and Invoice Verification Processing: If goods-receipt-based invoice verification configuration control is active for a particular order item, each invoice item can then be matched up uniquely with the goods receipt item especially in the cases where the delivery is expected to be made and posted in several parts i.e. partially delivery is expected. This control prevents a user from entering an invoice against a purchase order for which no deliveries are recorded but at the same time It is important to ensure that the inherent risks in this process related to Accounts payable or unrecorded liabilities are carefully managed. Most ERP systems mitigate this risk by recording inventory receipts in an un-vouchered receipt listing account that shows a detailed listing of received items but not yet invoiced and subsequently recording vendor invoices in the accounts payable subsidiary ledger when the invoice is received.

Preventing duplicate payment of vendor invoices: Creation of an internal document or a voucher for every vendor-to- invoice match and automatically assignment of control numbers for important documents like receivers, checks etc. are two of the important steps in preventing duplicate payment of invoices.

Application control considerations for Financial Reporting Cycle:-
Financial Reporting is one of the important processes within an ERP system and hence all the risks inherent in sub processes shall be addressed with proper controls at place. Some of the risks are:

1. Configuration of chart of accounts and closing of the financial books.
2. Journal entry configuration and Account Reconciliation.
3. Posting tolerances and account balancing (debits equal credits).

Some of the financial controls are:

1. Using workflowin SAP, proper authorization is achieved as two different users can be assigned to park and post a FI document.
2. Account reconciliations**:** This control shall be taken as a detective control i.e. all the errors shall be identified and corrected before filling SEC reports. A company shall make sure that all the accounts, including the new one, are included. Company shall adhere to the reconciliation policy. Proper instructions to carry out the reconciliation process with point of contacts shall be listed and proper documentation should follow.
3. Clearing tolerances shall be configured. It will clear documents only if the difference between accounts is within certain range and journal entries above pre-entered threshold are blocked i.e. not allowed to be posted to general ledger or sub-ledger accounts.

Access Security Controls:-
Access security controls is another area that aims to ensure that the organization's personnel are able to perform only those activities that are necessary to discharge their job responsibilities and help an organizationto appropriately segregate conflicting duties. The primary risks relating to access security involve giving unnecessary, unauthorized or excessive access resulting in unauthorized transactions and degradation of the integrity of the application data involved. Henceforth, access controls should be properly defined and implemented in an organization.

Segregation of Duties:-
Segregation of Duties (SOD) is a crucial aspect of access control environment because it not only helps in fraud prevention but also helps in alignment between IT and the business. Across an enterprise there are various functions and these functions are performed, together by set of roles and responsibilities. SoD says that the set of roles/responsibilities in an enterprise shall be assigned in such a way that any individual should not have end-to-end access rights over any function. Every company strives for zero SoD conflicts and for that it shall understand and try to reduce the current conflicts to the extent possible and apply mitigating controls to the remaining issues. Our approach suggests the use of SoD conflict matrix that includes the corresponding risk statement related to each conflictthat can help a firm to gain an understanding on the scope of sensitive transactions that are essential for company's key business processes. Some of the most critical segregation of duties conflicts in SAP, which includes both incompatibilities of transactions as well as fraud risks for SOx compliance, is listed below:

1. CR04 Process CRM Sales Order + SD02 Delivery Processing: In order to cover up an unauthorized shipment, a user could create a fictitious sales order if SOD is not implemented.

2. CR04 Process CRM Sales Order + CR07 CRM Billing: No SOD in place can result in false creation or modification of sales documents and generation the corresponding billing document in CRM.
3. SR01 EBP / SRM Vendor Master + SR03 EBP / SRM Invoicing: Same personnel of the organization can create a fictitious vendor and can enter an invoice to be included in the automatic payment run if SoD is not in place.
4. FI03 Bank Reconciliation + SR03 EBP / SRM Invoicing: An organization personnel user can hide differences between bank payments and posted Accounts Payable records.
5. SR01 EBP / SRM Vendor Master + SR07 EBP / SRM PO Approval: This conflict explains the fact that the same person can modify existing vendor master data and approve purchases to this new vendor

Table 1:- SOD-Conflict Matrix "Self-Compiled"

Business Process ↓ / **Roles** →	**Create Vendor**	**Change Vendor**	**Post Goods Receipt**	**Post Payment**	**Process Inventory**	**Goods Issue**	**Maintain PO**
Create Vendor		✖	✖	✖			✖
Change Vendor	✖		✖	✖			✖
Post Goods Receipt	✖	✖		✖	✖	✖	✖
Post Payment	✖	✖	✖			✖	✖
Process Inventory			✖				✖
Goods Issue			✖	✖			
Maintain PO	✖	✖	✖	✖	✖		

STEP 5- Documentation:-

According to SOX section 404, documentation is one of the crucial steps as it actually proves the existence of internal controls in the companyhence all the controls (application, access, entity) needs to be documented and tested ; needs to be remediated if found ineffective and documented finally to ensure that the company has a comprehensive system of internal controls which enables them to consistently report complete and accurate financial information for all of their key business transactions. Although the documentation of internal controls includes: Detailed Process description, Process flowchart, Business risk assessments, Risk Control Assessments, our approach considers Risk and Control matrix as one of the important tool for documenting the processes because it tells us about applications impacting the business process and a helps a firm in developing a matrix of key application control consideration. Following Risk Control Matrix takes into account few application controls from the three cycles as a basis for its formation.These forms are generated in duplicates and sometimes, in triplicates in order to send a copy to every party involved. These documents are very important during audits, queries, tracking of transactions etc. Hence, it is very important to devise an efficient and effective documentation system.

Table 2:- RISK-CONTROL MATRIX "Self Compiled"

Controls / Risks	Entering all NON-PO invoices in the system within 3 days of month end to maintain accounts payable	Purchasing Invoices can only be entered into the system for automatic matching if a valid PO and receipt are already in the system.	Unmatched PO invoices are forwarded to purchasing for follow-up	Reviewing of All purchase orders and non-PO invoices and making sure if they are authorized in accordance with company policy.	Reviewing of Cycle counts that result in a difference from perpetual Quantity outside limits set by thecompany; also items with a variance deemed to be material are recounted.
If purchases are in proper accounting period?	Preventive Control				
If invoices, prices and quantities are correct.?		Preventive Control	Preventive Control		
Recording duplicate purchases?		Preventive Control	Preventive Control		
If inventory records reflect proper quantities and amounts?				Preventive Control	Detective Control
If inventory counts, compilations and descriptions are accurate?					Detective Control

STEP 6-Using Continuous Auditing as a Meta Control:-

After identification and documentation of key application controls and risks, we have introduced continuous auditing in our approach. Continuous auditing is a method used to perform auditing activities, such as control and risk assessments automatically and on a more frequent basis. Also, technology plays a key role in continuous audit activities. Continuous auditing provides an additional level of controls to the existing controls as the auditor according to the internal audit plan of a firm can turn continuous audit processes on and off based on current system loads by reconfiguring the existing activities To facilitate continuous auditing we propose use of a prominent IT framework i.e. eXtensive Business Reporting Language (XBRL). It consists of identifying tags that are attached to items of data which can be processed efficiently by the computer. Also XBRL is easily extensible and can be used across platforms and software formats. This paper refers to the Continuous Auditing Web Services model (CAWS) by Murthy and Groomer and is further extended with the use of XBRL to address the mandates of SOX. Our ERP incorporates both the XBRL general ledger taxonomy and the internal control taxonomy that helps in achieving sustainable compliance according to SOX 404.The new XBRL-based ERP system has continuous auditing functionality that enables the company to continuously comply with SOX in a cost-efficient way as the financial reporting process becomes more efficient and economical.

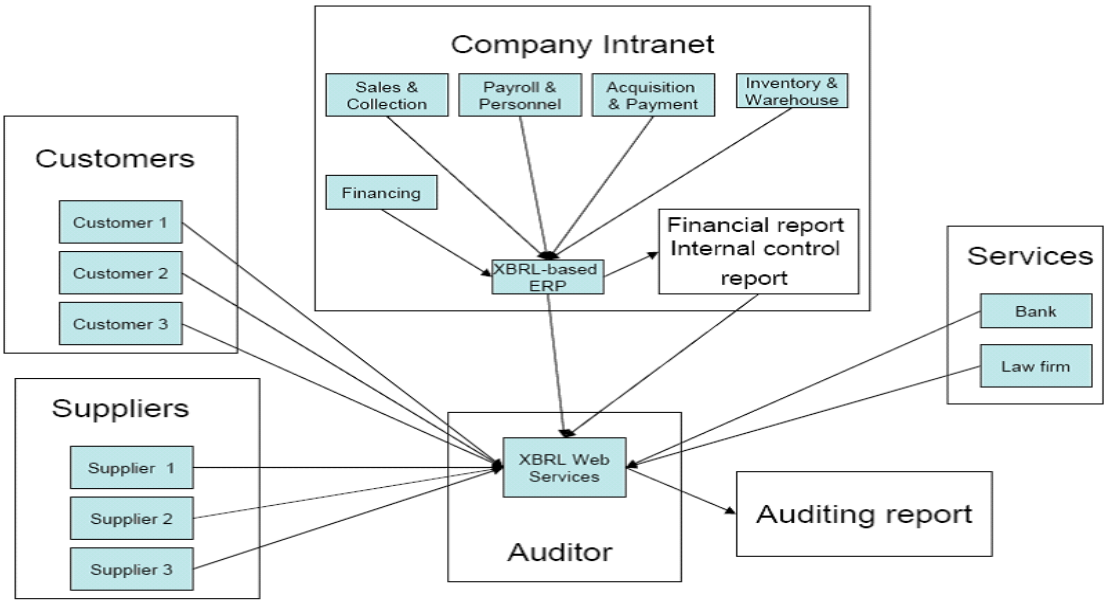

Figure 1:-The proposed XBRL-based ERP system
Real-Time Monitoring Tasks and Solutions [10]

Step 7- Testing:-

Testing Entity-level controls:-

To test the efficiency of entity level controls, combination of testing techniques i.e. use of enquiry, inspection/walkthroughs, observation and re-performance shall be used to conclude about operating effectiveness of internal controls.For example, the tracing of purchasing of a capital asset from the PO (beginning point) to the inclusion of the same on the financial statements helps in ensuring required approvals were met, categorization of asset was achieved and required policies were applied.

Testing Application Level Controls:-

Application controls, as discussed, are the controls that reside within the application and are applicable to individual transactions. There are various ways to test application level controls such as manual testing, semi-automated testing and automated testing. Although every process has its own pros and cons , our approach advocates semi-automated and automated testing for this purpose as manual testing is a very time consuming process and costly too. Semi-automated testing involves extraction, transformation and loading of data tableswhich is then brought forward for analysis which serve as evidence that a particular set of controls has been configured in a particular fashion. Automated testing isthe only way achieve operating effectiveness of an internal control procedure is to test every instance of it running. It can be achieved through Computer Aided Audit Tools also called audit data analysis. They can help an organization in: Reducing risk, improving efficiency as running a couple of data analysis tests on a full report can be done in seconds. Also, by automated testing we can actually test every instance that a control operates and hence it adds much greater value to our organization.For instanceby CAAT, a firm can test up to 600,000 payments compared to 50 samples taken by an auditor in case of manual testing and hence can easily find number of open issues. The reliabilityof IT controls testing falls intothree tiers:

Lowest reliance:-

It includes self –testingdone by the IT department of a company, the auditors consider it to be least independent and less effective.

Medium reliance:-

Internal Audit team performs a set of well-definedtests to show the compliance of each keycontrol. If Standard work paper format and strict adherence to the testing guidelines are practiced by the internal auditors, cost of external auditing can be lowered.

Highest reliance:-
at this level, the external auditors works independently and try to find out if significant gap exists in their findings or Internal auditors/IT testing teams. If significant variance is found, then unpleasant consequences might follow.

STEP8- Addressing Control Failure:-
The penultimate step according to our approach for a firm to abide by Sox 404 compliance is assessing the strength of internal controls in place, and hence external auditors takes into account the work of IT testing team, internal auditors and their own work and weak controls are compensated by strong controls(automated or manual) but when the control fails, the result or outcome is placed in one of the following three levels. They are: Deficiency, Significant Deficiency, and Material Weakness.

Deficiency:-
Application control deficiencies are generally tackled by performing a gap analysis of the control that is operating ineffectively and propose an action plan to close the gap in order to prevent financial misstatements. For example, if auditors notice that the requirement for approval for a critical process to complete was not included as an automated process in change management, it is remediated by putting controls as setting reminder mails and escalating the matter until the request is approved.

Significant deficiency:-
Significant deficiency occurs whenan important control is not working and the organization is not able to process or report its financial data accurately and henceforth the data is no more compliant with GAAP. However, a single significant deficiency may not result in SOX 404 deficiencies might. For example an auditor found more than 1 instance where there was a distortion in revenue and inventory recorded for the same period. Since the distortion was not material at the organization level, hence it was not a material weakness and was remediated by giving access of the document to a limited number of users which is a part of routine as access rights are modified on a continuous basis.

Material weakness:-
A deficiency or a combination of deficiencies becomes material when there is a reasonable possibility that a material misstatement of the company's annual or interim financial statements will not be prevented or detected on a timely basisi.e.one or more control will result in a 404 failure. For example, if auditors find that magnitude of financial misstatements because of any deficiency would be material and also the compensating controls proposed were not effective, then that financial misstatement arising from an internal control deficiency or deficiencies suffices the definition of material weakness.

STEP 8: Auditor's Report:-
It is proposed that after the end of fiscal year, the external auditors review the results of remediation tests and render an opinion on the effectiveness of the current internal control framework in place.It is deemed to be effective if financial inaccuracies and material misstatements of a company can be corrected by the internal controls put in place.The paper hence proposed COBIT as an IT governance model as it not only allows identifying controlling and evaluating all the IT processes but also supports the organization business processes and enables risk reduction and a controllable SOA implementation. To further improve the efficiency of SOx 404 implementation, the SOA/XBRL layer was also included in our approach that serves as a Meta control for auditors resulting in more flexible, connectable and aligned to the business processes information systems thus improving the reliability, efficiency and quality in financial reports issues. The following figure and table lists out a preliminary framework of few crucial controls with over 30 touch points for the auditors to consider in order helping them perform effective audits in accordance with SOx 404 compliancein Enterprise Resource Planning (ERP) systems.

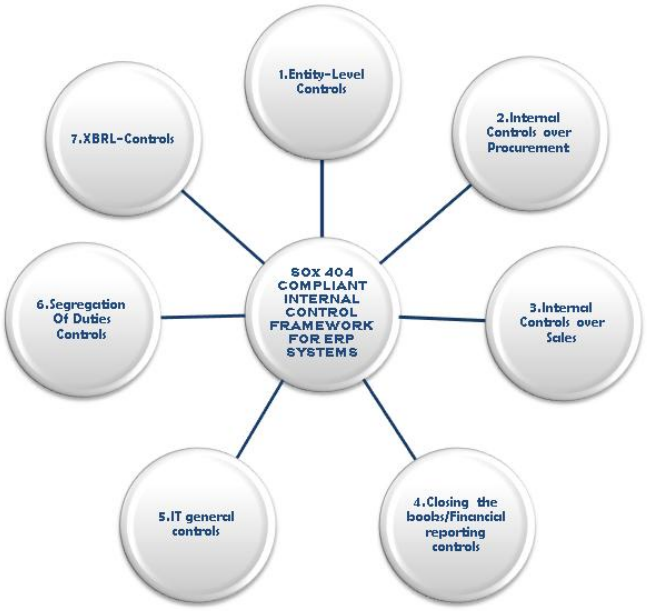

Figure 2:-Internal Control framework for ERP system**according toSOx 404compliance.**"Self-Compiled"

Table 3:- SOx 404 compliant Internal control checklist "Self-Compiled"

Controls	**Touch-Points to consider**
Entity-Level Controls	• Whether mission statement has been established and communicated to financial reporting staff. • If financial reporting processes and objectives have been defined by the management. • If a process has been established to identify and obtain all necessary consents and other legal documents prior to the issuance of the financial statements? • Is periodic review made to ensure employees in positionsof trust are bonded in amounts required by statutes ororganizational policy?
Internal Controls over Procurement	• If 1-way, 2-way and/or 3-way matching has been established to validate purchasing transactions? • If an invoice-numbering guideline is being adopted to avoid duplicate payments. • If Non-PO invoices are entered at the month end to maintain Accounts Payable. • If copies of receiving reports are sent directly to purchasing, accounting, and inventory record keeping? • If access to vendor master data is limited to employees authorized to make changes?
Internal Controls over Sales	• If sales order entry form have all the mandatory fields without which it cannot be further processed • If a system or a manual control exists to identify duplicate sales order. • If a control exists to automatically block the orders, if customer's credit limit exceeds. • If a control exists to check no modification of shipping date happens until approved by appropriate levels of management. • If cross validating segments in key flexfield exists to check for accurate billing, invoicing and payment processing.
Closing the books/Financial reporting controls	• If account reconciliation such as sub-ledger to general are automated as this would reduce any scope of manual errors. • If Clearing tolerances are configured i.e. the difference between accounts is within certain range and journal entries above pre-entered threshold are blocked i.e. not allowed to be posted to general ledger or sub-ledger accounts. • If park a post approval exists as a journal entry configuration approval?
IT general controls :	• If centralized automation of controls exists as it reduces the chances of manipulating the controls.

• Physical Access and Security • Logical Access Processes • Backup and Recovery • Disaster recovery policies • Software development processes • Configuration and Change management	• If written policies relating to controls over the physical security and access to the computer/server room exists? • Whether controls related to issuance, maintenance and termination of passwords exist? • If written procedures and controls exist for authorizing any change. • If procedures for emergency change exist? • If appropriate documentation is maintained for a period back up process. • If critical files are regularly copied to tapes so that they can be made available if a disaster happens. • Whether arrangements with vendor exist in case a disaster occurs.
Segregation Of Duties Controls	• Whether responsibilities for the disbursement approval function adequately segregated from those for the disbursement, voucher preparation and purchasing functions? • If responsibilities for initiating and approving transactions segregated from those for detail accounting, general ledger, reconciliation and other related functions? • If Purchase requisitions are reviewed and approved by someone other than the personnel initiating the purchase requisitions and these employees should not be able to modify the Vendor Master File • If responsibilities for authorizing vendor invoices and payments are segregated from recording invoices in the cash disbursement system.
XBRL-Controls	• Reviewing the details of the taxonomy to determine whether they are up-to-date with current business and reporting requirements and if the consistency of tagged data elements with the requirements of the taxonomy being used. • If there is an approval process in place that describes how financial statements shall be created from tagged data for inclusion on Web sites.

References:-

1. She-I Chang and Derek Jan, "SOX 404-compliant ERP System Internal Control Framework - The Preliminary Outcome," Journal of Business and Policy Research, vol. 5, no.2, pp. 282 – 295, December 2010.
2. She, W. and B. Thurasingham, "Security for enterprise resource planning systems," vol.16, no. 3, pp. 152-163.
3. Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements Available at:http://www.protiviti.com/en-US/Pages/default.aspx, accessed on May 2016
4. Ten Steps to Sarbanes-Oxley Compliance Available at http://www.ittoday.info/Articles/Ten_Steps_to_SOX_Compliance.htm, accessed on June 2016.
5. Maxim Chuprunov, "Controls in Financial Accounting, "in*Auditing and GRC Automation in SAP*, 1st ed. Berlin, Germany: Springer, 2013, ch.8, sec.8.1,8.2 pp. 189-202.
6. Brazel, J. F., "A measure of perceived auditor ERP systems expertise: Development, assessment, and uses", Managerial Auditing Journal, vol. 20, no.6, pp. 619-632.
7. Control objectives, management guidelines, maturity models in COBIT 4.0 Available at: https://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf, accessed on April 2016.
8. Cerullo, M. J., "The internal auditor's role in developing and implementing enterprise resource planning systems", Internal Auditing, vol.15, no. 3, pp. 25-34.
9. Groomer SM, Murthy US., "Monitoring high volume transaction processing systems using a continuous sampling approach", International Journal of Audit,vol.7, no.1, pp. 3– 19, March 2003.
10. Y.Li, Joseph N. Roge, Les Rydl, Jerald Hughes, "*Achieving Sarbanes-Oxley compliance with xbrl-based erp and continuous auditing*," Vol.8, no. 2, 2007.
11. Six Steps to an Effective Continuous Audit Process Available at: https://iaonline.theiia.org/six-steps-to-an-effective-continuous-audit-process, accessed on May 2016.

Acknowledgment:-

This research was supported/partially supported by **System Security and Cyber Forensics Lab**, **Ritsumeikan University, Japan**. I would like to thank my Professor **Mr. Tetsutaro Uehara** from Ritsumeikan University, who provided insight and expertise that greatly assisted the research. I would also like to express my deepest appreciation to all those who provided me the possibility to complete this report. A special gratitude I give to my project mentor, ***Prof. Pradnya Purandare***, whose contribution in stimulating suggestions and encouragement, helped me to coordinate my project especially in writing this report.I am also indebted to my alma mater ***Symbiosis Centre for Information technology***and our Director ***Dr. Dhanya Promod***. It is only because of the education imparted to me during the course of first year that I was able to settle and appreciate the experience gained during my 3 month stay in Japan.