Journal of Theoretical and Applied Information Technology
30th September 2015. Vol.79. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

APPLICATION INTEGRATION AND AUDIT CONTROL IN ORGNISATIONAL MERGER: CASE OF OMAN

SAQIB ALI, RAFI ASHRAFI AND SALIM AL BUSAIDI

Department of Information Systems, Sultan Qaboos University, Oman

E-mail: saqib@squ.edu.om; rafi@squ.edu.om; m20840@student.squ.edu.om

ABSTRACT

Information and information systems are valuable assets of today's organisation. These organisations use various applications based on their needs. Whenever there is a merger between two organisations, one of the biggest challenges is to integrate and audit those applications in the merged organisations. This paper reviews various application integration and audit frameworks, discusses their limitation, and proposes an approach for the post-merger integration and audit of the applications of the merged organisations. The approach is demonstrated through the application of a case study of the merger among three organisations in Oman.

Keywords: *Application, Business Process, Business Applications, Input Controls, Process Controls, Output Controls, Information Security, IT Audit, IT Governance, Oman*

1. INTRODUCTION

Corporate mergers and acquisitions (M&A's) are used as a tool for the corporate growth strategy and a way to form a stronger competitive organisation [1-4]. Many organisations have effectively executed mergers and acquisitions (M&A's) in the past, but the percentage of successful mergers and acquisitions (M&As) have been around 50% [5, 6]. Information System plays a vital role in the realisation of the value from M&A[7]. It has been discovered that IT related issues form the third most cited cause for failed M&As whereas about half of the forecasted benefits from an M&A are directly dependent on the integration of Information Technology (IT) [8][1, 9].

A number of researchers have established that they have a limited understanding of the role of IT in M&As [10-12]. It has also been discovered that the research domain concerning IT integration in M&As is in bits and pieces, and is scattered in various directions. Moreover, significant gaps also exist in the depth of the knowledge available [10, 13, 14]. Therefore, it has been strongly argued that there is an academic need to address this issue about the implications of M&A for IT integration approaches[13].

As the M&A arrangements are getting more complicated, the technology and the people involved in the M&A are gaining further importance since they form the key driver of the process for M&A. For an efficient and smooth M&A process, an early stage planning of information and communication technologies (ICT) for the integration process is vital for successfully obtaining the benefits of the M&A process [15].

As most organisations are dependent on IT to carry out their business activities, they cannot function effectively post-acquisition until the IT of the acquired business unit is integrated into the acquirer's IT infrastructure [10].

The rapid growth of the businesses is accompanied by a "phenomenal growth of information-based services and online systems" [16]. The growing recognition of information is evaluated by its ability to facilitate the creation of the organisational intellectual capital [16]. Hence, IT integration is preeminent as a big challenge [17] which plays a very significant role and is counted as a valuable organisational asset. The Information which Information System possess may be at a risk of being accessed, changed, and deleted without a tangible trace [18, 19]. Therefore, a proper and effective Information Systems (IS) governance and control is vital to safeguard the organisation's information assets.

The objective of Information Systems Controls and Audits is to determine the extent of their compliance with the organisations and legal policies, procedures and plans, as well as the extent to which the IS resources are protected and safeguarded from various risks and exposures. [20].

IT Governance and audit is an important aspect in protecting the organisation's information assets [21]. The development of the concept of IT auditing started during the mid-1960s. The advancement in technology and its incorporation into the businesses has led to numerous changes in the IT auditing concept. Taking care and securing the data of an organisation is a critical task since the information costs huge amount of money and thus immense amount of efforts is required to manage the organisation's information.

IT audit, also known as information systems (IS) audit, is the examination of the controls within an IT infrastructure of a given organisation [22]. IT audit conducts an evaluation, which helps to determine whether the assets are being protected, data integrity is maintained and effective operations are being executed by the IS. This helps verifying if the organisation's goals and objectives are being achieved. IT audit may be conducted in conjunction with standard audits like financial statement audit, internal audit, or other forms of attestation engagement.

Nowadays, organisations are required to meet the international standards in doing their businesses in order to compete efficiently at a lower cost and provide better quality of products and services. In order to achieve these goals organisations need to improve their business processes, standards and frameworks constantly. This is pursuant to the world-wide trend that has increased demands of IT governance, audit and control.

The numbers of merged organisations have increased over the past few years. Merger and Acquisition has become a popular business activity because of its various benefits, but it has created new challenges in terms of the integration of the merging businesses' applications. It is desirable that this integration is based on rational criteria and the applications follow a governance framework to ensure business strategy alignment and compliance with the government requirements.

A number of organisations have implemented and combined various governance and audit frameworks to integrate and audit merged applications. This research attempts to review the IT governance and application audit and controls frameworks specifically used for companies where integration and collaboration is required. This study provides guidelines, proposes different frameworks and recommendations for the application audit to be adopted for the integrated applications in the merger companies. The next section reviews some of the important and relevant concepts reported in the literature.

2. LITERATURE REVIEW

2.1 Information Technology/ Systems audit and controls

An audit is an assessment, examination and review of the organization's policies, procedures, processes and management activities that must follow a set of guidelines and standards imposed by an external authorised body [23]. According to the David Browns report, [24] the organisations which are planning mergers, should take attentive portrayal of the pros and cons involved in merging the information technology systems. Most of the organisational activities processes, management and workflows depend on information technology, and therefore, the IT needs to be monitored and audited. Information technology audit can be defined as *"the process of collecting and evaluating evidence to determine whether a computer system is designed to maintain data integrity, safeguard assets, or allows organisational goals to be achieved effectively, and uses resources efficiently"* [25]. IT is used in almost all business functions and processes of the organisations in which software's, hardware's and systems vary from different vendors, as some are developed in-house and some outsourced. This has increased the business risk and imposed a strong need for IT audit and review. According to Valstybes Kontrole [19], following are some of the most common reasons to perform IT Audit:

- unsatisfactory turn out of the auditing around the computer, in order to obtain a better data reliance
- insufficient and highly questionable dependency over the controls
- lesser possibility of an effective enforcement of the security for information and data
- the booming and quick advancement of the information technology
- ease of accessibility of the organisation IT resources like network and PCs
- the increased growth of hackers

The ultimate goal of the IT audit is to substantiate a constant, permanent and endless accessibility of the system to the authorised users, providing them with a reliable, accurate and consistent data. In addition to auditing the information technology, it needs to be controlled and monitored, which will support having IT governance. IT controls consist of policies, procedures, practices and organisational structures. These are devised to ensure that the business objectives using the IT are achieved, and the undesired events are prevented or detected and corrected [26]. Information systems are an integral part of the corporate information technology, and they need to be audited as well [27]. There are general and application controls for the information systems. The general controls include controls of the software development cycle, maintenance and security. On the other hand, the application controls are to ensure having a proper user's accessibility, data accuracy, and validity of transactions performed through applications and systems.

2.2 Application Audit and Controls

Application audit is part of the IS auditing. However, it is auditing of a single application at a time, for example, auditing Human Resources Management System in the ERP system. The application audit can even be extended to audit the application database, servers and operating systems. There are three types of application controls. First is preventive control, where a proactive approach is adopted to prevent errors from happening, second is detective control in which errors are found and corrected whenever they appear and third is the corrective control where it is learnt from an oversight, identifying the cause and then take corrective actions, and accordingly amend procedures and processes of the application.

The application audit should ensure that there are controls in the following areas [28]:

- **Administration:** This area focuses on general control about the ownership of the application. Better controls on the application result in a stronger control over the other application control areas as well. For example, the application owners make sure that the roles and responsibilities of the application users are defined as per their job responsibilities, which are derived from their respective job profiles.
- **Inputs, Processing and Outputs:** This area is all about the procedures and processes of the data entry on the applications, methods to process them and the data usage. For example: the transactions' data that is entered in the system should be validated followed by the formulas and processes. Next the result should be recalculated to ensure its accuracy followed by the distribution of the output or reports to the authorised users and finally the effectiveness of these reports should be guaranteed and confirmed. Furthermore, report reconciliation is done frequently to ensure that the application process output is consistent and correct.
- **Logical Security:** This area is about access control in which the application owner appoints a custodian who is responsible for adding, reviewing and deleting application users [29]. For example, if an employee is transferred to a different department, his/her access to the application is modified accordingly as per the new job profile.
- **Disaster Recovery Plan:** In this area, there is control over the backup policies as well as the offsite storage of the backup. Its purpose is to mitigate the effects of any potential disaster.
- **User Support:** This is to ensure user support to control risk. There are documentations for the applications like user manuals, help documents or online help.
- **Change Management:** This is to avoid or minimise the impact of the application changes on the system security, integrity and Service Level Agreement (SLA). Furthermore, this helps in providing a stable production environment by planning and coordinating the application changes properly. Furthermore, a change in any application should be aligned with the current processes and procedures [30, 31].
- **Third Party Services:** This is to ensure that the third party service is meeting the business requirements and objectives of the application. Furthermore, the vendor is required to follow the company rules and procedures. Moreover, the third party service agreements are reviewed by the legal department.

2.3 IT Governance

IT and its associated risks and requirements for control over the information are important elements of the organisation governance. The structure of relationships and processes to control the organisation in order to achieve the enterprise's goals is called the IT governance. The goals are achieved by adding value to the business while balancing the risk versus return over IT and the related processes. IT governance results in an efficient and effective enhancement in the organisation's processes [32]. IT governance is important for making sure that the investment in IT generates the value reward and reduces the risks, and avoids failure. A successful governance framework makes sure that IT investments are aligned with the organisational goals.

As per PricewaterhouseCoopers (PWC) [33], there are a number of elements that need to be considered when forming or evaluating an IT governance. They are not limited to, but include:

- **Structures and roles:** where all the tasks and activities should be delegated to individuals or teams

- **Processes:** the development of all activities that require producing products or delivering services.
- **People:** to make sure that competent and potential staff is available with the required skills, knowledge and experience, to support and handle the IT applications and services effectively and efficiently.
- **Controls:** to ensure that the processes of IT are delivered efficiently and are aligned with the organisation's requirements
- **Technology:** the availability of the right technologies in terms of software or hardware or any other technological tools to support IT services
- **Metrics:** measurements of the people, processes, technology and controls to ensure continuous improvement of the IT governance

The Institute of IT Governance [34] has identified five focus areas that describe the important things that management should address while governing the IT in the organisation. The five focus areas are:

- **Strategic alignment:** to create a link between the business strategy and IT so that they can work well together
- **Value delivery:** to ensure that IT departments in the organisations deliver the goals that are established and promised at the beginning of each application investment
- **Resource management:** to manage the organisation resources effectively from which the staff management will be utilised more efficiently
- **Risk management:** the development of a risk framework by having some strict IT measures that manage risk
- **Performance measures:** a methodology for business performance management like IT Balanced Scorecard which checks if the IT contributes in achieving the organisation goals

The following section presents the discussion on IT and Application audit frameworks. This includes COBIT, ITIL and ISO/IEC 27001 frameworks. In this research a real case study of the mergers of three organisations, Oman Oil Refinery Petroleum industries (OMAN OIL RPI) is presented. A brief profile of each company, its auditing methods, frameworks, processes and problems faced will be discussed in Section 4 and 5. Section 6, presents the post-merger application integration. Where section 7, discusses the auditing of the new company applications. Last section of this research presents the recommendations and conclusion.

3. REVIEW OF IT AND APPLICATION AUDIT FRAMEWORKS

IT Audit in general and the application audit in particular, is a complex process and is critical to enhance the efficiency of the operations of the information technology. There are several IT and application audit frameworks, and it is difficult to determine and select which framework is suitable for the organisation's IT functions and strategies [35]. The majority of organisations use in-house developed frameworks for auditing their IT applications. The statistics shown in Figure 1 by IT Industry Survey [34] highlights the preferences of the audit frameworks for the studied organisations.

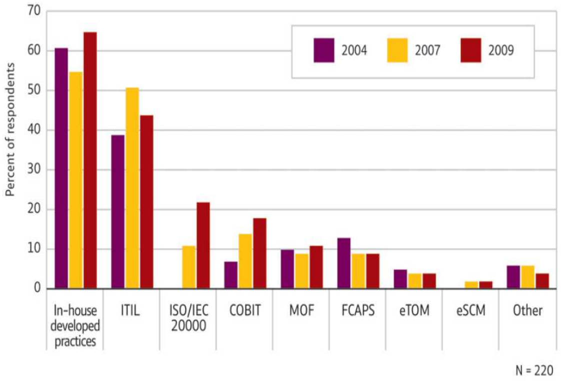

Figure 1: Preference Of The Audit Frameworks (Adopted From [34])

Figure 1 shows that a significant number of organisations use in-house developed practices/ frameworks, followed by ITIL, ISO/IEC 2000, COBIT, MOF, FCAPS and others. Perhaps the reason seems to be that most of the off-shelf frameworks do not fulfill the requirements of those organisations. Also, the focus of each framework is different. Therefore, no framework fully satisfies the needs of the organisation.

In the next sections, a brief review is carried out on main characteristics, features and components of the selected IT Audit and Control frameworks.

3.1 COBIT

The main objectives of COBIT are to ensure that the managers and auditors of a given organisation implement the set of general information technology control objectives that are internationally accepted. COBIT had started in 1996 [36]. It stands for Control Objectives for Information and Related Technology. The COBIT was designed by ISACA to ensure proper governance and control over the IT's day to day activities. Furthermore, it helps the IT decision makers to close the gaps between control requirements, technical issues and business risks.

The latest release of ISACA is COBIT 5. COBIT 5 is merged with COBIT 4.1, Val IT 2.0, IT risk frameworks [37] and also encompasses various standards and frameworks which are; (1)The open group architecture framework (TOGAF), (2) Information technology infrastructure library (ITIL), (3) PRINCE2, (4) International organization for standardization(ISO), and (5) Project management body of knowledge (PMBOK) [38]. COBIT 5 escorts five principles which are; Principle 1: meeting stake holder's needs, Principle 2: Covering the enterprise end-to-end, Principle 3: Applying a single, integrated framework, Principle 4: Enabling a Holistic Approach, and Principal 5: Separating governance from management [39]. These principles of COBIT 5 allow the organisation to frame an effectual management and governance framework that improves efficiency of the information and technology investment and use for the benefit of stakeholders.

There are around 290 generic COBIT objectives, and they are grouped into six COBIT components, which are executive summary, framework, control objective, control practices, management guidelines and audit guidelines. The COBIT framework has four domains, which are:

- **Plan and organise (PO)**: In this domain strategic IT plans are developed to sustain the organisation business objectives.
- **Acquire and implement (AI):** The developed plans in the first domain might require the organisation to acquire new applications, or develop new skills for the employees to execute the plans and make sure that they are aligned with the business objectives. Furthermore, the acquired applications need to be implemented, tested and maintained.
- **Deliver and support (DS)**: This phase makes sure that the applications perform as per the user requirements or as expected from the implementation, and carry on performing over the time as per the expectations.
- **Monitor and evaluate (ME)**: This phase uses the service level agreements or the baseline scope of work of the application implementation in order to help the IT managers grasp and perceive as to how the actual performance is compared to the expectation. This also aids the IT managers to be preventive.

These four domains are organised and controlled by COBIT, and those controls are identified based on best practices. COBIT also provides audit guidelines to evaluate the application controls and see if they are compiled [40]. A global overview of the IT processes of an organisation is provided by COBIT. This is achieved by focusing on controls and metrics of the IT. It also provides a common language for the organisation's manager to communicate the goals and results with the auditors and IT professionals.

3.2 ITIL

ITIL stands for: Information Technology Infrastructure Library (ITIL). ITIL is a public framework which defines the best practice in IT service management. It is issued by the office of Government of Commerce, UK. It is not a standard but rather a wide range of good practices that need to be implemented by organisations. It provides a framework for the governance of IT and focuses on the ongoing improvement of the quality of IT products and services provided both from a business' and a customer's perspective [41]. It provides wide knowledge and skills about IT governance. ITIL breaks down the information technology functions into different components called services (Life cycle approach). These services have three levels [40]:

- **Strategic:** long term goals of the provided service at the IT function and having high level activities that are required to achieve the goals
- **Tactical:** all the processes to perform the tasks and activities that are needed to be performed to deliver the services
- **Operational:** the actual execution of the processes to deliver the services to the users

By focusing on the practices of service strategy, design, transition, operation and continual service improvement, ITIL follows the approach of Life cycle for the organisation's IT services [41].

The service strategy is the collaboration between business strategists, and IT functions in the organisation so as to develop IT service strategies, which help and support the organisation's strategy. The service design is about designing the overall IT architecture of the organisation plus the IT services in order to meet the customers' business objectives. Service transition is controlling all the changes from the development environment into the production IT environment. This includes the new development and or the changed application in IT services. The service operation is about delivering and supporting operational IT services in a way that meets the organisational business needs and benefits. The continual service improvement is learnt from the past and others experience. It also adopts an approach that ensures continuous improvement of IT applications and services.

3.3 ISO/IEC 27001

ISO/IEC 27001 is a framework, created for information security management and it is an internationally recognised structured audit framework. It defines a process that can be implemented to evaluate, implement and maintain the information security management system (ISMS) in the organisations. Information security management system(ISMS) consists of the following nine elements: (1)Application information security, (2)Application security, (3) Application external security, (4) Application user access, (5) Application physical security, (6) Application operational security, (7) Monitoring application security audit, (8)Application use access management, and (9) Application processing security. Information security management system (ISMS) elements are discussed in later section. ISMS framework also provides an inclusive set of controls that consist of best practices in information security. ISO 27001 is a universal framework and can be applied to all industry sectors. Its main emphasis is on the prevention of risks and attacks. ISO 27000 has many series, which are:

- ISO 27000 – principles and vocabulary (in development)
- ISO 27001 – ISMS requirements (BS7799 – Part 2)
- ISO 27002 – ISO/ IEC 17799:2005 (from 2007 onwards)
- ISO 27003 – ISMS Implementation guidelines (due 2007)
- ISO 27004 – ISMS Metrics and measurement (due 2007)
- ISO 27005 – ISMS Risk Management
- ISO 27006 – 27010 – allocation for future use

ISO 27001 gives the organisations the best practices for their information security management. ISO 27001 has 11 control areas:

- Security Policy
- Organisation of information security
- Asset management
- Human resource security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development, and maintenance
- Information security incident management
- Business continuity management
- Compliance

The physical, technical, procedural, and personnel security must be balanced by the management systems. A closed loop approach is used by the ISO 27001 which is, the Plan, Do, Check, Act (PDCA) cycle model. The PDCA model is also implemented in various other management systems within the ISO such as those defined within ISO9001 (Quality) and ISO14001 (Environment).

- **PLAN- Establish the ISMS:** The plan of an organisation could be the need to establish security policy, objectives, targets, processes and procedures which would enable to manage the risk and improve the information security. This would deliver the results that are in accordance with an organisation’s overall policies and objectives.
- **DO - Implement and operate the ISMS**: The plans like security policy, controls, processes and procedures are implemented in this step.
- **CHECK -Monitor and review the ISMS:** After the implementation, the organisation needs to assess and measure the performance security policy, controls, processes and procedures. The organisation should report the issue to the management in order to take the corrective actions.
- **ACT - Maintain and improve the ISMS:** This deal with taking the corrective and preventive actions that are resulted from the management’s critique to achieve continuous developments and improvement of the ISMS.

4. CASE STUDY: OMAN OIL REFINERIES AND PETROLEUM INDUSTRIES:

This section presents a case study of the merger of three oil and gas organisations in Oman. To achieve anonymity they are referred as:

- Company X
- Company Y
- Company Z

4.1 Company X

Company X is a limited liability company which was established in 2007. The company was formed as a result of the merger between the two well-known companies. The ownership is shared between the government of Oman and Oman Oil Company on 75%-25% basis approximately. The Government of Oman is represented by the Ministry of Finance. The company X processes

Oman's export blend crude to produce Liquid Petroleum Gas, Regular and Premium Gasoline, Kerosene/Jet A-1, Diesel, Long Residue/Bunker Fuel Oil, Propylene, Naphtha, Low-Sulphur Gas Oil, Fuel Oil and Granulated Sulphur. After supplying a sufficient amount of fuel to Oman through local marketers, the remaining products are marketed internationally. The company X has obtained various ISO certifications over the years. Those certifications are ISO 9001:2000, ISO 14001:2004 and international occupational health and safety management system specification (OHSAS 18001:1999). The Refinery was also awarded ISO 27001:2005 for Information Security Management System. Integrated Management Systems (IMS) was implemented at this refinery in early 2000s.

4.2 Company Y

Company Y was established as a company, which would construct and own a petrochemical complex. The ownership of company Y is shared among with other three companies. The commercial production of company Y commenced in 2010. Para Xylene and Benzene, two of the important raw materials for a variety of consumer goods are the major products of company Y. Since company Y is a newly formed organisation and the systems are still under development, it is yet to obtain certification from ISO for various standards.

4.3 Company Z

Company Z is one of the world's leading manufacturers of polypropylene. The polypropylene is supplied to the other companies, who use it to produce many products. Approximately 80% of the company is owned by the government of Oman. The company's production started in 2006. Company Z has ISO 14001:2004, OHSAS 18001:2007 and ISO 9001:2008 certifications.

5. CURRENT SITUATION AND PROBLEM DEFINITION

5.1 The Applications in the merged companies

Company X is a dominant company among the merged companies in terms of revenue, number of employees, plant facilities, latest technologies and number of applications and databases. Company X has around 50 applications and more than 20 databases to manage. Some of the applications share one database, and these applications are fully integrated and interfaced. The BIMS (Business Information Management System) is the largest application in company X, and it is an integration of different applications such as Financial, HRMS, Oil accounting, purchasing and inventory. Furthermore, each refinery has its own plant information systems in two locations; however, all of the data is then transferred and processed in the BIMS in order to get a fully integrated information system. Company Y is the second largest company but doesn't have integrated applications. Currently, their databases are based on Microsoft office excel and access the plant information system as it is associated and developed during the plant construction, and is vital to the operation. Company Z, which is the smallest company, has integrated applications under SAP. SAP has different modules like HRMS, Payroll, Finance, KPI, Purchasing and Inventory. Furthermore, company Z has the stable plant information system.

5.2 Application audit

Since company X is certified Information Security Management System (ISO 27001:2005), it is following the practices of the ISO 27001 on auditing the applications and IT in general. However, there is no clear and formal framework to conduct the application audit. As a matter of fact the application audit is conducted once a year to satisfy the government and certification requirements. In the application audit, the auditor will have a checklist and will interview the audited that could be the end user or the IT functions as employee and will check if the application processes, databases, procedures and security guidelines are in line with the checklist. Due to the absence of the formal application audit framework, many issues and problems have occurred in the company; some of these issues are reported by the specialised external application auditors which are mentioned below.

- **Confidentiality:** The responsibilities of the users are not reviewed frequently and therefore, some users have access to applications which are not related to his/her job. For example, an employee who has been transferred from the HR department to a purchasing department may still have access to the HR system.
- **Integrity:** The employee's information is maintained and updated in different applications like HRMS, Financial and Purchasing. Any update in one of these applications will not be reflected on the others. For example, if an employee is terminated on HRMS application, the employee will not be terminated in Financial and Purchasing modules automatically and hence will need to be terminated manually.

- **Availability:** Because there is no periodic maintenance plan, and because of the instability of the application, the application servers and services need to be restarted and therefore, the availability of the applications is reduced, which affects the end users' day to day activities.
- **Security:** Many roles and responsibilities in the application are not as per the employee's job profile and also there is no access level control. This has affected the ownership and accountability of the application.
- **Input, processes, output of the application**: This is because there are no data entry procedures in the applications. Furthermore, the processes within the application are not as per the business processes and procedures which might result in the incorrect outcome which, consequently, will lead to wrong reports and decisions.

While investigating the company X, this research found out that there is no formal audit process for auditing the applications, and this is because the Internal IT auditor in the company doesn't have proper audit skills and qualifications. Furthermore, the senior management is not involved in the preparation and execution of the audit, and therefore, the audit is not taken seriously by the audited employees. However, the final findings and the recommendations for the corrective action is communicated to the senior management in a formal meeting, and all line managers attending this meeting.

As for the other two companies, they have an audit department, but no formal internal audit mechanism is in place for the applications. Since the government has the highest shares of both the companies, the state audit of Oman conducts the audit, including the application audit to ensure the compliance as per the government's requirement. Due to the lack of audit practices in these two companies, it has been found that the same issues pertaining to company X are related to company Y and company Z also.

Having the unified audit policies, procedures and framework for the application of the new company require integration and consolidation of the applications. Therefore, the management of the new company Oman Oil and Refinery Industries has to take action to integrate and centralise all the IT functions under the shared services' division. All the three companies need to have one application infrastructure with unified policies and procedures. The next section will discuss the application integration approach of the three companies.

6. POST-MERGER APPLICATION INTEGRATION

The ultimate goal of integrating the application is to maximise the benefit by collaborating and consolidating the processes and functionality of the IT application as well as eliminating redundancies of both the applications and databases. There are four strategies to integrate the application which is unification of the applications, select the best, interface and new development.

6.1 Integration of the applications:

The applications of the dominant company (company X) will be considered as the standard to be applied to the other companies. This means all users of the merged companies will be using all the applications of company X, and hence their applications will be replaced and not be used, even if these applications have components and features that are better than the application in use. The data and processes of the other companies will be migrated into the main application. This might lead to some resistance from the other companies' users, and thus they will need to be trained on using the new applications so that the transition could be smoother. On the other hand, this approach will lower the risk and will reduce the cost and time of new implementation.

6.2 Selection of the best application among the three companies

In this approach, the best applications of the three companies will be selected and used for the new company. The problem in this approach is the agreement among the three companies on the selection criteria since each company sees that their application is the best among all. Furthermore, this type of approach requires interfaces among the selected applications and will relatively increase the cost and implementation time.

6.3 Interface the existing applications of the three companies

In this approach, the applications of all companies will be operated in parallel. Most probably the interfaces among the applications will be minimised. This approach can be implemented in a timely manner with lower integration cost, but there will be no synergy within the three companies' applications.

6.4 New application development

In this approach, all the existing applications of the three companies will be eliminated, and the new company will develop new applications from scratch. The new applications will be developed based on the old applications with enhanced features on the processes and procedures of the new company. This approach is very expensive and time consuming. Table 1 summarises the different application integration approaches and illustrates the comparative analysis of these approaches in terms of cost, time to implementation, approach, advantages and disadvantages over others.

Table 1: Summary Of The Different Application Integration Approaches

	Integration of the applications	**Select the Best Application**	**Application Interfaces**	**Develop New Application**
Approach	Select all the applications of the dominant company	Select the best applications of three companies	Keep and interface all the existing applications	Replace all applications and develop new applications
Implementation Time	Low	Medium	Low	High
Implementation Cost	Low	Medium	Low	High
Advantage	Low Risk, low effort	Higher users acceptance	Low effort	Higher users' acceptance, Low risk, enhanced capabilities
Disadvantage	Users' resistance, other good systems will be ignored	More interfaces, difficult selection	High risk, high operating cost, complicated	High effort and long project time

The new company can select one of the approaches based on their objectives behind the merger of the three companies. In addition, the selection could be based on the priorities, time frame and cost with the assurance of business continuity and maximum operational performance.

The selection and then use of the approach for the integration of an application depends upon the nature and size of the companies. If the companies are of small level, then the best approaches are: (1) - to select all the applications of dominant company and (2) - to keep and interface all the existing applications. The reason behind selecting these two approaches for small level companies is that these approaches have low implementation time, low implementation cost, low risk and low effort. While in the case of medium or large level companies this research suggests the two applications integration approaches which are: (1) – to select the best applications out of the three companies and (2) – to replace all applications and develop new ones. The above mentioned approaches are a best fit for the medium or large level organisations because of their enhanced capabilities, higher user's acceptance, low risk and high effort.

For the purpose of this research the best application integration approach is; selecting the best application out of the three companies. This is because, during the transition period of any given organisation, the management of the company most likely would select applications among the three companies as a temporary measure until all the processes and procedures are unified, practiced and proven to work smoothly. This decision is valid because there are good applications that are recently developed and tested in the three companies, and have been working smoothly. Moreover, it will be difficult to develop a new application for the new company where the operation and processes are still not unified and stabilised.

7. MERGER COMPANIES APPLICATION AUDITING

The integration of the applications of the merger companies will be in compliance with the audit and IT governance framework. This is to ensure that all the IT and its application strategies are in line with the organisation's strategy. The new companies may have a new application audit framework constructed from scratch or current framework could be modified to cater for the new changes of the integrated application. However, whichever framework is selected, it will ensure the following:

- All core business applications are reviewed in terms of access control, authorisations, validations, application business process and documentation such as manuals and procedures.
- Data integrity and reliability is ensured.
- The application system administration procedures and policies, security of operating systems and database security is reviewed.
- Application physical securities are also checked and monitored like server room access control, power supply, air conditioning and humidity monitoring and control.

- The framework is devised by the policies and procedures that will ensure the network security of internal and external connections to the system, firewalls, router access control lists.
- It has the policies and procedures for application maintenance, backup procedures and storage, availability of reliable disaster recovery/business continuity plan.

7.1 New audit frameworks

There are three proposed application audit frameworks for the new company. These frameworks are based on how complex the applications are, and how they are integrated and will be functioning on the new company. The proposed frameworks are: application risk based audit, ISO 27001 and combination of COBIT and ITIL. Following are the details of each proposed framework.

- **Risk based application audit:**

This approach is simple and easy to implement. It is not structured like COBIT, ISO 27001 and ITIL. Since the new company has a wide number of applications with different levels of complexities and functionalities operated and accessed from different locations, the auditors should know all the associated risks. The risk-based application approach is basically based on three points which are; 1) - understanding the application environment and business and technical processes associated with the application followed by 2)- examining and assessing the controls of these applications and then 3)- assessing the risks of these application controls. It consists of following phases:

- **Phase 1:** This phase is about understanding the application environment and business & technical processes. In this phase, the auditors should have a full understanding of the applications in terms of business process, inputs, processing, outputs, databases and applications interfaces. Moreover, it's about the understanding of application control environment, whether the application purchased is AS-IS or customised, hosted internally or with an external providers and also if it's built in-house or by a third party.
- **Phase 2:** This phase is about examining and assessing the controls of the applications, where the auditors assess the important application controls as follows:
  - Input controls, basically check the integrity of data entered into the application, method of data entry (i.e; whether it is entered manually or through data interface), and parameters and validations of the data input.
  - Process controls ensure that the data processed is as per the business processes. It also checks the formulas and if the process is done in a timely manner.
  - Output controls verify that the output result of the application matches with the intended result by processing the data manually.
  - Integrity controls check that the data entered and processed is consistent and correct.
  - Application tracking controls work as an audit trail to enable the identification of the transactions and events that are recorded in the application by tracking data entry and transactions.
- **Phase 3:** This phase is about application control risk assessment, where the auditors use risk assessment methodologies to identify the weaknesses of the application controls and identify the critical business functions and processes that will be affected by these application controls. After defining all the application controls, the auditors define the risks associated with these controls and weigh all these risks to show the level of importance of each control. After that the auditors conduct the risk assessment, rank all risks and perform the evaluation. Based on the evaluation, the audit can be planned.

The risk based approach will enable the management and the auditors to develop an effective application audit plan where all the weaknesses will be overcome and would propose enhanced controls to the applications.

- ***ISO 27001 (ISMS – Information Security Management System)***

The second approach is to have ISO 27001 for which the company X got a certification. This certification helped the company X demonstrating effective improved security controls. This has forced the employees to practice these security controls. Furthermore, this has reduced the cost by having a better risk management and more accurate cost benefit analysis and therefore, it eventually results in a good investment. The implementation of this framework requires the efforts of every single employee starting from the clerks to the top management leading to all the functions of the company. Adapting this framework will require re-implementation since company X is the only certified company and the other two are not. This is because the characteristics, assets and technologies used in the company X business are different from those of company Y and company Z.

The implementation of this framework starts with the planning. As matter of fact this phase is part of a continuous cycle which ensures that the correct components are engaged, evaluated, monitored and improved on a continuous basis. It uses the plan, do, check and act framework. The benefits of this cycle are improved security and its planning and ongoing protection information of the applications. The plan is to define the scope of the ISMS framework and define its policies.

7.2 Using ISMS to audit application in the new company

The ISMS can be used as an audit framework for the new company. This framework is more into the information security of the applications, and most of the proposed actions are related to the information security. This framework consists of the following elements:

- **Application information security**: The application information security policy is approved and reviewed by the management and it is ensured that this is communicated to the employees and contractors working in the company.
- **Application security:** In this framework the application security is clearly defined and the responsibilities are assigned to the application users. Furthermore, the confidentiality agreement is clearly defined and reviewed from time to time.
- **Application external security:** This is important when a third party from outside the organisation is accessing the applications. The risks associated with application external access are identified and evaluated.
- **Application user access:** The responsibilities have been identified and reflected on his/her access level of the application. Furthermore, any changes on the employee's responsibilities are immediately reflected on the access given. Moreover, if the contract of employees or contractors and third party is terminated then the access to the application is terminated immediately.
- **Application physical security:** This framework comprises of physical security to protect the application like allowing only the authorised staff to gain access and control over the application server room, securing the offices and any other facilities where applications are accessible and also ensuring physical protection against damage from fire, floods, and earthquakes.
- **Application operational procedures:** This is to ensure that all user manuals, technical manuals and coding and operating procedures are well documented and available to all users. Also, any changes in the management procedures are controlled, and duties and responsibility are separated from the users to discourage and lessen any unauthorised access to the applications. Another important point here is to separate the testing application instances from the production instances and keeping both of them in separate networks.
- **Monitoring application security audit:** All the application users' activities are logged to assist the auditors in order to conduct any investigations and monitoring application access control. Moreover, monitoring application activity usage is reviewed. Furthermore, user login faults are logged and analysed, and a required action is taken if necessary.
- **Application user access management:** Access management includes user registration, user identification and authentication, access level and password management.
- **Application processing security:** This is to ensure input data validation like having input error messages, and responsibilities for users to input data. In addition, the data output of application is validated.

This framework will help the management to realise the importance of having ISO 27001 by making them comprehend the risks affecting the company while integrating the applications of the merged companies and how ISO 27001 will resolve to overcome these risks. Not only that, the ISO 27001 requires to align with the corporate and new company's strategies with ISMS requirements and therefore, the involvement and commitment of the top management is required.

- ***COBIT and ITIL***

The third framework is a combination of the COBIT and ITIL frameworks. The purpose of this combination is to have a strategic alignment between the IT application and the overall organisational objectives. Furthermore, the combination will add value to the application services and cost reduction.

COBIT provides standards to control the organisation IT and its applications. It also ensures expansion of IT involvement in business processes and helps managing the application risk. Generally, COBIT framework identifies the things that need to be completed in IT in order to enable the organisation achieving its goals by setting up controls. Since COBIT is a control framework, it does not include process and procedures. It focuses on what the company needs to do but not on how it needs to do. ITIL, on the other hand, is a processing model for IT service management. It is built on best practices for IT and application service delivery and support.

The company can use the COBIT framework for the application and IT audit and the ITIL framework for IT services management and improvement. Since both are important and vital to the alignment of the applications with organisational goals, it is recommended that, instead of choosing either the COBIT or ITIL, the company combines them both. By doing this, company will have an integrated and effective framework and it is the most effective option. The new company as the governmental company, will meet the governmental audit requirements and controls. This can be achieved by having COBIT framework, to help the company in dealing with external vendors and have a better control and also adopting ITIL to streamline the processes and application service management for optimum utilisation. Therefore, both COBIT and ITIL will enable the new company to improve processes and align IT functions with business and audit requirements. Furthermore, COBIT framework identifies the applications' controls whereas ITIL framework identifies the best practices of the application management, processes and procedures.

8. RECOMMENDATIONS

Based on literature review and research findings, following are some general recommendations that need consideration in order to ensure a proper application audit using any of the proposed frameworks that can be implemented on the new merged company:

- The selection of the application integration is needed to be rationalised and aligned with the new company's overall objectives and business needs. The selected integration methodology will ensure that the business operations and day to day activities are effectively handled. Time and cost and users acceptance will also be balanced during the selection. This will help maximising the profit of the company.
- Ensure that the overall audit process is in compliance with the government audit requirements and practices. Furthermore, the internal controls of the applications are in place and tested to guarantee their compliance with the government laws and regulations. This will harmonise the application audit framework with the government requirements.
- Impose controls over the application inputs by having data input authorisation, preventing the duplication of data input and having data input validation. This will avoid the entry of unauthorised, irrelevant, incomplete and duplicate data and will result in system integrity.
- Impose application processing controls by validating input and generated data, finding out and detecting the errors and have proper transfer of data from one processing stage to another. This will avoid the inaccurate processing of transactions. The application control will help the company to ensure valid, complete, accurate and auditable transactions process.
- Impose application controls on output to ensure that output is complete, accurate and correctly distributed to the concerned people. This will help having the output distributed on time and reconciled with input and process parameters. Moreover, this will help to increase and enhance the confidentiality of the output. The output files need to be protected in order to reduce the risk of unauthorised changes.
- The audit framework and auditors should consider the following controls after the application integration is completed:
  - Control assessment of the application business processes
  - Application security assessment
  - Application data conversion and interfaces controls

- The applications should maintain reports such as the menu report, active users report and active responsibility report. This will help the auditor to identify the application menus and those accessing them from the active user list using certain privileges. This verification can be checked along with the organisation chart of the company and job profile of the employee.

9. CONCLUSION AND FUTURE WORK

Technology is advancing at a very fast pace and so the companies' operations are becoming more complex, consisting of thousands of processes. Thus, the need of the time for the companies is to implement the technologies to make their services more effective and efficient. Information technology audit is playing an important role in optimising the business process and ensuring that IT is in compliance with international IT governance standards. IT audit frameworks are very important for the alignment of organisational objectives. This research has reviewed information technology governance frameworks and has proposed an approach that best fits the newly merged company, resulted from the merger of company X, company Y and company Z. The new company has been proposed to select an application integration approach and thereafter select the audit framework that combines COBIT, ITIL and ISO 27001 frameworks. ITIL and COBIT are complementary, and they can be combined to work as an audit framework for the new company.

This research has reviewed and analysed various approaches to combine and consolidate different audit frameworks and to find out how they can fit and align into the organisational objectives of the merged organisation. Also it has evaluated the impact of adapting combination of different frameworks on the organisational performance and on the quality of the application audit.

10. ASSUMPTIONS AND LIMITATIONS

The research has been conducted solely on the three companies mentioned in section 4. One of the assumptions is that, these three companies have done the M&A procedure in the best possible manner, which may not be the case. Also the research is a regional one and may not be applicable internationally. The standards used to study the situation and recommendation have been used from the international organisations like ISO, COBIT, ITIL etc. and it is assumed that the organisations in Oman may also comply with the same perspective. But it is very much possible that there might be various differences in the approach and perspective of the organisations in Oman and elsewhere. The study has been conducted on a limited number of three companies and all being from the same field of Oil and Gas industry. The recommendations and observations provided by the paper may require revision when considering more number of companies from various other fields.

The authors have provided a study and recommendations for the M&A process. But these recommendations are yet to be tested and verified for efficiency and effectiveness. This can only be done when these recommendations are standardised and a merger takes place following those standards. Thus a further study and large scale implementation is required to verify the results of this research and consolidate the standards for the local market, which is a major need of the hour.

REFRENCES:

[1] 1. Henningsson, S., *Managing Information Systems Integration In Corporate Mergers And Acquisitions* In *School Of Economics And Management*. 2008, Lund University: Lund, Sweden

[2] 2. Turban, E. And L. Volonino, *Information Technology For Management*. 8th Ed. 2012: John Wiley And Sons, N.J. .

[3] 3. Junior, P.R., P.E.D. O, And A.F. Da Silva, *Mergers And Acquisitions: An Efficency Evaluation.* Applied Mathmatics, 2013. 4(1583-1589).

[4] 4. Haleblian, J., Et Al., *Taking Stock Of What We Know About Mergers And Acquisitions.* Journal Of Management, 2009. 35(3): P. 469.

[5] 5. Mehta, M. And R. Hirschheim, *A Framework For Assessing It Integration Decision-Making In Mergers And Acquisitions. In System Sciences*, In *Proceedings Of The 37th Annual Hawaii International Conference*. 2004, Ieee. P. Pp. 264-274.

[6] 6. Cartwright, S. And R. Schoenberg, *Thirty Years Of Mergers And Acquisitons Research: Recent Advances And Future Opportunities.* British Management Journal, 2006. 17.

[7] 7. Toppenberg, G. And S. Henningsson, *An Introspection For The Field Of Is Integration Challenges In M&A*, In *Proceedings Of The 19th Conference On Information Systems*. 2013: Chicago, Illinois.

[8] 8. Rodgers, M., *Stay Hungry*, In *Cio Magzine*. 2005.

[9] 9. Sarrazin, H. And A. West, *Understanding The Strategic Value Of It In M&A.* Mckinsey Quarterly, 2011.

[10] 10. Mehta, M. And R. Hirschheim, *Strategic Alignment In Mergers & Acquisitions: Theorizing Is Integration Decision Making.* Journal Of The Association For Information Systems, 2007. 8(3): P. Pp. 143-174.

[11] 11. Alaranta, M. And S. Henningsson, *Shaping The Post-Merger Information Systems Integration Strategy. In System Sciences*, In *Hicss 2007. 40th Annual Hawaii International Conference*. 2007, Ieee. P. Pp. 237b-237b.

[12] 12. Böhm, M., Et Al., *A Dual View On It Challenges In Corporate Divestments And Acquisitions*, In *32th International Conference On Information Systems (Aisel.Aisnet.Org)*. 2011: Shanghai, China.

[13] 13. Wijnhoven, F., Et Al., *Post-Merger It Integration Strategies: An It Alignment Perspective.* The Journal Of Strategic Information Systems, 2006. 15(1): P. Pp.5-28.

[14] 14. Henningsson, S., Carlsson, And *The Dysiim Model For Managing Is Integration In Mergers And Acquisitions.* Information Systems Journal, 2011. 21(2011): P. 441-476.

[15] 15. Holm-Larsen And Michael, *Ict Integration In An M&A Process*, In *Pacis 2005 Proceedings (2005):95, Aisel.Aisnet.Org*. 2005.

[16] 16. Buchanan, S. And F. Gibb, *The Information Audit: Role And Scope.* International Journal Of Information Management, 2008: P. Pp. 171-192.

[17] 17. Posnick, J.E. And J.A. Schoenborn, *Executives Report That Mergers And Acquisitions Fail To Create Adequate Value*. 2007.

[18] 18. O'donnell, J.B. And Y. Rechtman, *Navigating The Standards For Information Technology Controls.* The Cpa Journal 2005.

[19] 19. Kontrole, V., *Methodological Recommendations For Information Systems Audit.* Auditor Grenerals, 2006.

[20] 20. Pathak, J., *Information Technology Auditing An Evolving Agenda*. 2005: Springer.

[21] 21. Davis, C., M. Schiller, And K. Wheeler, *It Auditing: Using Controls To Protection Information Assests*. 2006: Mcgraw-Hill Osborne Media. 387.

[22] 22. M. Merhout, J. And D. Havelka, *Information Technology Auditing: A Value-Added It Governance Partnership Between It Management And Audit.* Communication For The Association For Information Systems, 2008. 23: P. 463-482.

[23] 23. Gallegos, F., Et Al., *Information Technology Control And Audit*. 2004: Auerbach.

[24] 24. Brown, D. *Don't Overlook It In The Merger.* . 2001; Available From: Http://Business.Highbeam.Com/411267/Article-1g1-75452258/Dont-Overlook-Merger.

[25] 25. Liu, Q. And G. Ridley, *It Control In The Australian Public Sector: An International Comparsion*, In *European Conference On Information Systems(Ecis)*. 2005.

[26] 26. Hein, R., *The Application Audit Process-A Guide For Information Security Professionals*. 2005: Sans Institute 2005.

[27] 27. Turban, E. And K. David, *Introduction To E-Commerce*. 2002.

[28] 28. Arkansas, S.O., *Physical And Logical Security*. 2006.

[29] 29. Leopoldi, R., *Change Management Methods And Implementation Best Practices*. 2002.

[30] 30. Itgi, *Cobit 4.1*. 2007, United States Of America: © 2007 It Governance Institute. Www.Itgi.Org.

[31] 31. Pricewaterhousecoopers, *It Governance Global Status Report-Excerpt*. 2004.

[32] 32. D. Schwartz, K. *It Governance Definition And Solutions*. 2007; Available From: Http://Www.Cio.Com/Article/2438931/Governance/It-Governance-Definition-And-Solutions.Html.

[33] 33. Nicho, M., *Information Technology Audit: Systems Alignment And Effectiveness Measures*, In *School Of Computing And Mathematical Sciences* 2008, Aut University Auckland, New Zealand

[34] 34. Blum, R. *It Industry Survey*. 2009; Available From: Http://Www.Ukessays.Com/Essays/Information-Technology/Discussing-The-Developments-Of-It-Services-Information-Technology-Essay.Php.

[35] 35. Isaca. *About Isaca*. 2010; Available From: Http://Www.Isaca.Org/About-Isaca/Pages/Default.Aspx.

[36] 36. Xansa, A.C., Et Al., *An Introductory Overview Of Itil® V3*. 2007: The Uk Chapter Of The Itsmf.

[37] 37. De Haes, S., R. Debreceny, And W. Van Grembergen, *Understanding The Core Concepts In Cobit 5*. Isaca Journal, 2013. 5.

[38] 38. Zhang, S. And H. Le Fever, *An Examination Of The Practicability Of Cobit Framework And The Proposal Of A Cobit-Bsc Model.* Journal Of Economics, Business And Management, 2013. 1(4).

[39] 39. Preittigun, A., W. Chantatub, And S. Vatanasakdakul, *A Comparison Between It Governance Research And Concepts In Cobit 5.* Iracst- International Journal Of Research In Management & Technology (Ijrmt) 2012. 2(6).

[40] 40. Arora, P., *Itil - It's Value To It Infrastructure Management Services*.

[41] 41. Kneller, M., *Executive Briefing:The Benefits Of Itil®, 2010, White Paper*. 2010.