Controls for information technology and reporting evaluation

Risk is a necessary undertaking for any business. Success in business is determined by effectively managing the risk. Effective risk management helps to protect the company from losses because of poor accounting practices and fraud. Good controls also protect company management from the liability when they certify the financial statements issued in the annual report because they are also certifying the internal controls. The internal control process begins with management and the attitude that management portrays through the company.

From this attitude, management gives direction, and the direction becomes policies and procedures. The policies and procedures build the structure of the internal controls environment. Automated information systems have expanded a business's ability to accomplish more work with fewer people; however automated information systems have also increased the risks business's face that use them. Automated information systems, specifically the IT infrastructure that supports the systems, have created a whole new group of threats and vulnerabilities to the internal control system.

To manage the risks of the automated information system, several standards have been developed to provide guidance on the implementation of controls. This paper provides an assessment of these control standards, and which options each standard provides. Vulnerabilities and Threats Automated information systems have become a critical component in the operation of modern business. The widespread use of personal computers and server infrastructure that had become prevalent over the last 50 years has fundamentally altered the way business is conducted.

This optimization has allowed more work to be done with fewer people and a much higher level of detail to be incorporated into the work through the algorithmic computational abilities of computers. However, these new systems have also provided new vulnerabilities to business operation. A vulnerability is any weakness in the accounting information system that exposes the business to additional risk (Raval & Fichadia, 2007). Vulnerabilities can come from different places. These places can be the design of the nfrastructure itself, the policies and procedures that support the infrastructure, and the users of the infrastructure. The first type of vulnerability in an accounting information system is the system architecture itself. Modern applications are usually composed of thousands of lines of code, which interface with other applications, other computers, and process information. With the scale of modern computer applications, it is nearly impossible to produce an application that is free from errors in the code, in which can expose the business to risk.

The applications that support the structure come from two different classifications. The applications can be custom built or off the shelf. Each of these types of applications has a different set of risks. Off the shelf applications are written to be robust enough that individual users can adapt the application to their specific business need. This robust nature of the application means that the code that composes the application is much more complicated then the code of an application tailored specifically for the business.

This increased complication provides additional opportunities for coding errors to create a weakness in the system. Custom built applications are simpler and streamlined to the specific business need, but as the business that creates the application is working on a project that will not be widely distributed, there is a risk that the business will not be in place to support the application once it is launched. The second component of vulnerabilities to an automated information system is the policies and procedures that the system implements for system security.

Policies and procedures govern all aspects of the system from user accounts, system access permissions, password change policies, restrictions on who can access, maintain, and update files, what applications can be deployed on individual computers, and on the system. The ability to install applications and modify system configuration is something that should be restricted to protect lay users from inadvertently exposing the system to a control risk by modifying or installing an application, or making a system change that should not be done. The applications themselves present another vulnerability for business.

Microsoft Excel and Microsoft Access are very convenient applications for data storage. These applications allow individual users the ability to generate powerful applications that are not in the direct control of the information technologies group. These applications can house critical business data in a format that is outside of the control of the company. The users of an automated information system represent the most significant vulnerability to the system. If the programmer is successful in developing air free code, it will do little good if the user enters inaccurate information.

If a company develops sound policies and procedures for the operation of an accounting information system, they will be of little benefit if the policies and procedures are not implemented and followed. The user of an automated information system is both the largest beneficiary of the results of the system and also the most likely component of the system to compromise the system. Compromising the system can be done through intentional fraud, or through unintentional errors that were not captured.

Options for Internal Controls Three different internal control schemes have been developed by various international bodies to assist organizations in developing and maintaining adequate internal controls for their automated information systems and information technology infrastructure. The Control Objectives for Information Related Technology (COBIT) have been produced by the IT governance institute, and are considered the standard for Information technology security and controls. The International Standards Organization has released ISO 17799, which extends British standard BS 7799 for the protection of information assets.

The final widely recognized organization that has produced a standard for automated information systems controls is the Committee of Sponsoring Organizations (COSO) (Raval & Fichadia, 2007). COBIT approaches IT controls from a process perspective. This control structure identifies 34 high-level control objectives that have been divided among five different key frameworks. The control objectives cover acquiring infrastructure applications and software systems, the installation of software and infrastructure, and the management of both users' access, and hanges to the system (Raval & Fichadia, 2007).

ISO 17799 is an extension of the British standard, BS 7799. Both standards divide the control aspects into two different categories, the management of data and the management of operations (Raval & Fichadia, 2007). The management of data consists of all activities used to validate, secure, and process the information contained in an automated information system. This includes activities such as system backups and validation of applications as well as review of the existing data to ensure its accuracy.

The Committee of Sponsoring Organizations has released a comprehensive framework for internal controls that consists of five components, risk assessment, control environment, control activities, information and communication, and monitoring (Raval & Fichadia, 2007). Risk assessment is the evaluation to identify anything that has the potential to prevent an organization from reaching their objectives. The control environment consists of both the tone the company has for internal controls and the strength of the policies and procedures that are in place to mitigate risks.

Control activities are policies and procedures as well as their implementation that a company uses to reduce the risks of failing to meet a business objective. Information and communication control both how business information is moved through the company, and how policies and procedures are distributed out to the employees. Monitoring is the final component of the COSO framework. Monitoring effectively reviews all activities to ensure that the control environment is appropriate, policies and procedures exist and are followed, and the risk assessment is up-to-date and current.

Evaluation of Control Options The three control frameworks COBIT, ISO 17799, and the COSO framework all provide effective models for the implementation of internal controls. The COBIT framework is the most detailed framework, but it focuses specifically on information technology and not on all aspects of the accounting information system. ISO 17799 provides the same specific functionality as COBIT, but focuses on the information system and not necessarily the IT system. Both of these standards provide a framework but do not offer ways to implement the framework.

The COSO provides a generic model for implementing a framework that covers a broad base of business applications. However, it lacks the detail of the other frameworks (Raval & Fichadia, 2007). All three frameworks provide strengths and weaknesses for the implementation. COBIT and ISO 17799 are functionally interchangeable with their applications being very similar with a different focus. For optimal results with simplification of the implementation, either of these frameworks could be implemented with a concurrent implementation of the COSO guidelines.

The COBIT or ISO 17799 would provide the framework for the implementation, and the COSO guidelines would provide the implementation plan for that framework. Conclusion The widespread use of computerized business application in the modern business environment has created a new classification of risks and accompanying internal controls. These risks focus on the vulnerabilities to an automated information system that are created by the system design itself, the policies and procedures that support the system, and the users who use the system.

Because of these risks, three different internal organizations have developed control frameworks to assist companies in mitigating the business risks from automated information systems. These three frameworks are COBIT, ISO 17799, and COSO guidelines. These three frameworks are not mutually exclusive, and the best benefit from these frameworks can be provided by using either the COBIT or ISO 17799 for the framework, and the COSO guidelines to support the implementation of the framework.