Concordia University College of Alberta

Master of Information Systems Security Management (MISSM) Program

7128 Ada Boulevard, Edmonton, AB

Canada T5B 4E4

A Conceptual Framework for the Prevention and Detection of Occupational Fraud in Small Businesses

By

Lisa D. A. Yearwood

A research Paper submitted in partial fulfillment of the requirements for the degree of

Master of Information Systems Security Management

April 2011

Academic Advisors:

Dr. Dale Lindskog, Assistant Professor, MISSM

Dr. Shaun Aghili, Assistant Professor, MISSM

Dr. Pavol Zavarsky, Director of Research and Associate Professor, MISSM

Ron Ruhl, Director and Assistant Professor, MISSM

A Conceptual Framework for the Prevention and Detection of Occupational Fraud in Small Businesses

By

Lisa D. A. Yearwood

Academic Advisors:

Dr. Dale Lindskog, Assistant Professor, MISSM

Dr. Shaun Aghili, Assistant Professor, MISSM

Dr. Pavol Zavarsky, Director of Research and Associate Professor, MISSM

Ron Ruhl, Director and Assistant Professor, MISSM

Reviews Committee:

Dr. Pavol Zavarsky, Associate Professor, MISSM

Dr. Dale Lindskog, Assistant Professor, MISSM

Ron Ruhl, Assistant Professor, MISSM

Concordia University College of Alberta

Information Systems Security Management

7128 Ada Boulevard, Edmonton, AB

Canada T5B 4E4

A Conceptual Framework for the Prevention and Detection of Occupational Fraud in Small Businesses

By

Lisa Denyse Ann Yearwood

123186, ladyearwood@hotmail.com; ldyearwo@student.concordia.ab.ca

904-614-1959

A research paper submitted in partial fulfillment of the requirements for the degree of

Master of Information Systems Security Management

Academic Advisors: Dr. Dale Lindskog, Dr. Shaun Aghili, Dr. Pavol Zavarsky, Ron Ruhl

April 2011

Contents

A Conceptual Framework for the Prevention and Detection of Occupational Fraud in Small Businesses

Lisa D. A. Yearwood, Dale Lindskog, Shaun Aghili, Pavol Zavarsky, Ron Ruhl
Concordia University College of Alberta
ladyearwood@hotmail.com,
{dale.lindskog,shaun.aghili,pavol.zavarsky,ron.ruhl}@concordia.ab.ca

Abstract

This research paper develops a conceptual framework for internal control, suitable for small business owners, to guide the effective selection and implementation of internal controls that help prevent and detect occupational fraud. Although the de facto internal control framework, the Committee of Sponsoring Organization's (COSO) Internal Control – Integrated Framework (1992), appears to be suitable for large businesses, this research argues that it is unsuitable for small businesses, due both to the resource constraints of small businesses, and the design and intended purpose of the COSO framework. The conceptual framework is risk-based, allowing small business owners to tailor it to their environment in order to ensure that their specific risks are addressed. It also employs a defense-in-depth approach by improving confidentiality, integrity and availability at various levels by highlighting preventive, detective and corrective controls in administrative, operational and technical layers.

Keywords: Occupational fraud, small business, fraud prevention, fraud detection, security, internal controls.

1. Introduction

This research seeks to develop a conceptual framework suitable to guide small business owners in the selection and implementation of internal controls to help prevent and detect occupational fraud. The framework, which is risk-based, has been designed as an alternative for smaller businesses with less resources. It can serve as both an internal control framework and a template for crafting an internal audit plan. This will in turn encourage smaller businesses to start implementing and maintaining an internal audit activity designed at providing better controls over occupational fraud related threats. The framework allows small business owners to tailor it to their environment and to provide defense against fraud by looking at individual targets, determining their perceived critical characteristics and then selecting appropriate controls.

Fraud is defined as the "wrongful or criminal deception intended to result in financial or personal gain" [**1**]. In their 2010 Report to the Nation (RTTN), the Association of Certified Fraud Examiners (ACFE) emphasizes that fraud is a global problem for organizations of all sizes, but that small organizations are disproportionately victimized. The report suggests that this may be due in large part to a lack of anti-fraud controls, as compared to their larger counterparts, since a comparison of such controls at small businesses with those at larger businesses showed that the small businesses did in fact have fewer internal controls in place. Further, the primary weakness contributing to occupational fraud in small businesses was cited as a lack of internal controls [**2**].

1.1. COSO Overview

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework, Internal Control – Integrated Framework, has been recognized as the de facto standard for internal controls, based in large part on the fact that the Securities Exchange Commission (SEC) of the United States has recommended it for compliance with Section 404 of the Sarbanes-Oxley Act of 2002 (SOX) [**3**]. COSO defines internal controls as a "process, effected by an entity's board of directors, management and other personnel, designed to assure reasonable assurance regarding the achievement of objectives in the following categories: effectiveness and efficiency of operations, reliability of financial reporting and compliance with applicable laws and regulations" [**4**].

The COSO framework was designed as an evaluation framework to guide in the assessment of internal controls selected, designed and implemented by an organization's management. It has, from the inception of its recommended use for SOX compliance, been a cause of concern for small public companies, as evidenced by the outcry from the small business community and the resulting compliance extensions requested through the US Congress and granted by the SEC; initially until April 2005 and more recently until June 2010.

The stated objectives of the report and by extension the framework are "to assist management in improving their entities' internal control systems and to provide a common understanding of internal control among interested parties" [**5**]. The framework has achieved these objectives, and is viewed as an important tool for the assessment of internal control in large businesses. These objectives, however, presuppose that management has already selected, designed and implemented what they consider to be effective internal controls. For many small businesses, this is generally not the case, and in instances where it is, management's determination of the "effectiveness" of the implemented controls is based on the individual controls, and not on a holistic view of their environment or internal controls. COSO does not provide a list of possible controls that small business should consider when looking at their environment, and where it does deal with controls specifically, in the "Control Activity" section, it is written from an assessment perspective and provides no selection or implementation guidance.

1.2. Small Business Constraints

The ACFE defines a small organization as one with fewer than 100 employees and while the COSO does not specifically give a definition of a small business it does use the term "smaller" and provides characteristics of smaller companies. In this paper a small business is one with fewer than 100 employees where its leadership has significant ownership interest, and limited financial, time and expertise resources.

Welsh and White observed that a small business is not a little big business and underscored this point by noting that "the very size of small businesses creates a special condition – which can be referred to as resource poverty – that distinguishes them from their larger counterparts and requires some very different management approaches." [**6**] The resource constraints they highlight are time, financial and expertise constraints. Time constraints exist because there are less staff members and therefore fewer man-hours available and, therefore, there is little time available for activities outside of the normal job activities for individual employees. There is also a time constraint on the managers who exercise control, oversee day to day operational activities and make personal interventions where necessary. [**7**] "This lack of time and the centrality of the owner in the small business's daily activities may act as a further barrier to accessing useful formative know-how." [**8**] Financial constraints refer to the limited amount of finance available, and that which is available is used for the normal operations of the business. Because of this constraint small business management will, when absolutely imperative, choose the cheapest available solution to a problem, which may not really solve the problem at all, but may rather compound the issue by providing a false sense of security. Finally, the expertise constraint refers to the limited expertise within the small business. While this constraint is generally a direct result of financial constraint, it is important enough for the purpose of this paper to be given separate mention. Small businesses generally lack the necessary in-house expertise to provide proper guidance on issues of importance, such as finance, technology and security, and it is therefore common for small businesses to rely on external consultants for the provision of these services.

In addition to the constraints above, argued by Welsh and White, there is a noted difference in the characteristics of management and the knowledge acquisition in small businesses, when compared to larger businesses. In small businesses, management tends to rely on heuristics- which are short-cuts in decision making - when they do not have all the relevant information or when decisions are not based on fully objective criteria. The use of heuristics to respond to uncertainty, as well as the generation of knowledge via learning how to resolve and overcome thresholds, suggests that the processes whereby knowledge is generated, applied and transferred relate to the immediate managerial context and task environment [**9**]. Fraud does not fall into either the "immediate managerial context or the task environment", as the management is generally unaware of the occurrences of fraud and, as Herbane states, "where threats are known and expected (such as computer failure) plans are developed. In contrast, if a threat is not known or expected (or is ambiguous and not fully understood), the threat is less likely to secure attention in terms of formal planning." [**8**]

A review of the internal controls that the ACFE examiners found in place at small businesses suggests that some small business owners are aware of the need for internal controls, but, due to the lack of specific guidance for the selection and implementation of controls, they implement controls without any formal planning. As a result they

may have ad hoc controls in place without regard to the holistic mitigation of the threats in their environment. Given the absence of specific controls in the COSO framework and the further lack of implementation guidance, this framework is unsuitable for the resource impoverished small businesses. Currently, the effective selection and implementation requires a certain expertise that will often be lacking in the small business context. Without the necessary expertise to inform the selection and implementation process, it is likely that the current ad hoc implementation of controls will continue. Expertise requires money and, as noted, this resource is also constrained. Knowledge can be generated by research, but this requires time, yet another constrained resource. Therefore, the first requirement for any control framework targeted specifically at small businesses is that it must offer them a list of controls so that they can select those that best suit their individual environments. The second requirement therefore is that the recommended framework should be a risk-based approach that is easily customized to individual organizations, based not only on their specific risks, but also on their available resources. The third requirement for the framework is that it must provide for prevention and detection of frauds and also, where necessary and possible, the correction of the consequences of the detected frauds. The framework described in this paper can be used by small businesses to assist them in ensuring that they select and implement internal controls that will provide a measure of defense in depth to their identified risks.

In the next section a description of the framework is provided as well as assessment, selection and implementation guidance, in order to provide effective solutions against fraud in the small business environment. In section 3, there is a discussion of the limitations of the framework. Finally, in Section 4, conclusions are provided as well as potential future work that can be carried out to assess the effectiveness of the framework.

2. The Proposed Framework

2.1. Overview of the Proposed Framework

A framework is a real or conceptual structure intended to serve as a support or guide for the building of something that expands the structure into something useful. A conceptual framework is a set of ideas or concepts organized in a manner that makes them easy to communicate to others. The purpose of the framework proposed in this research is to clearly describe to small business owners a structure to guide them in the prevention and detection of fraud in their businesses. It achieves this by drawing concepts familiar to information security practitioners and uses them as the pillars for the development of a fraud prevention framework to assist small business owners in their attempt to mitigate fraud.

The framework described in this research places the asset or process to be protected at its center, as shown at Figure 1 in Section 2.2. The specific asset or process is then analyzed to determine whether the confidentiality, integrity or availability of the asset is its critical characteristic, as described in Section 2.2. Once the critical characteristic or characteristics have been determined, controls are then selected from the list of controls at Appendix 1 and implemented to give the protection that the asset or process requires. The controls provided are classified primarily as administrative, operational or technical controls, where administrative controls generally take the form of policies and procedures, operational controls are implemented as actions that should occur to ensure that compliance with the policies is maintained, and technical controls are controls that are implemented by the system. The controls are also simultaneously classified as preventive, detective or corrective. Controls should be selected after giving consideration to the type of control required, in conjunction with the type and placement of other controls.

The controls provided in the list of controls at Appendix 1 have been chosen due to the ease with which they can be understood and implemented, especially in the small business environment. In addition to separating the controls as described above, the list also highlights which potential frauds the control can be used to mitigate. Finally, the list provides some implementation guidelines to assist business owners in the effective implementation of the controls. The guidelines given are non-specific, as each business will be different and therefore implementation will also be different.

The frauds that have been used in developing the framework have been selected from the frauds that were highlighted in the ACFE RTTN 2010 report. Two additional categories of frauds which were not covered by the RTTN have been included as their omission, especially in a computerized environment, could have dire consequences to business. These two additional categories are the destruction of data and social engineering. A broad description of these frauds is provided in Table 2.

2.2.The Conceptual Framework Explained

The purpose of the framework is to assist small business owners in preventing and detecting fraud, by assisting them to select and implement controls in an effective and efficient manner. Small business owners and managers, with their plethora of backgrounds, are generally not well versed in risk management practices, and therefore, the framework needs to use language that could be easily understood by them, while still presenting a structure and set of guidelines for them to use to make judgments about effective control selection and implementation. In order to achieve these objectives, the conceptual framework consists of a graphical representation showing the target at the center of a segmented circle, as pictured in Figure 1. The target can be a specific piece of information, a system or a process. The remainder of the circle is divided into thirds representing the CIA triad where confidentiality is concerned not only with preventing unauthorized entities from accessing the system or process under consideration, but also with ensuring that authorized entities do not access items that they are not specifically authorized to access. Integrity is concerned with ensuring that the target is accurate in all stages of its life, and, therefore, that only authorized entities are entitled to make authorized changes. This notion is important as all entities that are authorized to make changes may not be authorized to make all changes, but rather, may only be authorized to make specific changes. Availability is concerned with authorized entities being able to access the parts of the system that they are authorized to access, during the hours when they are authorized to access it.

The CIA circle has three concentric circles superimposed on top of it, with the smallest providing the target at the center, as discussed above. Radiating outwards the concentric circles further divide each third into three sections providing layers and affording the opportunity to offer defense in depth. This defense in depth will be from a control perspective where controls are defined as safeguards or countermeasures [**10**]. Moving away from the target being protected, the layers are categorized as technical, operational or administrative, with each respective layer being represented by the next concentric circle. Technical controls are the controls "that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system." [**10**], and as such, technical controls generally form the innermost layer of protection. Operational controls are countermeasures that are "primarily implemented and executed by people (as opposed to systems)." [**10**]. The administrative controls are controls "that focus on the management of risk and the management of information system security." [**10**], and they usually take the form of organizational policies and procedures. The controls will also be simultaneously categorized as preventive, detective or corrective, with the view that if a specific control fails to prevent a fraud, the fraud should be detected in as short a time frame as possible. Based on the criticality of the process targeted by fraud, once fraud detection occurs, controls may be needed to correct the consequences of the fraud.

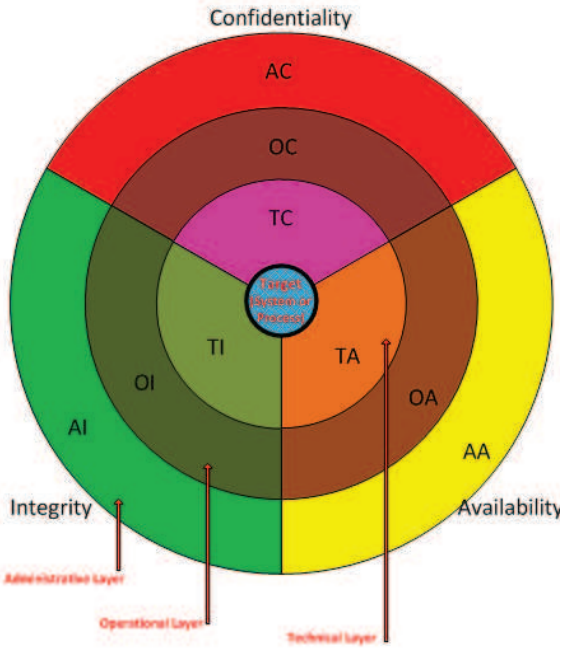

Figure 1 – The framework with the target system to be protected

The framework takes each of the three information characteristics and provides possible controls at each of the three layers, providing nine separate segments surrounding a center target which the business owner deems as vulnerable. The business can then select suitable controls for the desired segments in an effort to minimize the potential for fraud against that target. The nine separate segments of the framework are as follows:

Table 1 – The control segments of the framework

Administrative	AC	Administrative controls designed to protect the confidentiality of a target system.
	AI	Administrative controls designed to protect the integrity of a target system.
	AA	Administrative controls designed to protect the availability of a target system.
Operational	OC	Operational controls designed to protect the confidentiality of a target system.
	OI	Operational controls designed to protect the integrity of a target system.
	OA	Operational controls designed to protect the availability of a target system.
Technical	TC	Technical controls designed to protect the confidentiality of a target system.
	TI	Technical controls designed to protect the integrity of a target system.
	TA	Technical controls designed to protect the availability of a target system.

The framework provides a list of controls (Appendix 1) that can be used to assist in the mitigation of fraud. The list includes preventive and detective controls, as well as a few corrective controls to be used in circumstances where prevention fails. The list, while not exhaustive, is comprehensive enough to allow small business owners and managers to select appropriate controls that fit their environment, taking into account their specific resource constraints. The controls have been taken from both the ACFE 2010 RTTN, and the National Institute of Science and Technology (NIST) Special Publication 800-53A. The list is divided into administrative controls, operational controls and technical controls and it provides information on whether the specific control can be used as a preventive, detective or corrective measure; whether it addresses the confidentiality, integrity or availability of the system; which common frauds it can address, taken from the ACFE list of commonly occurring frauds, as well as social engineering and the destruction of data (defined in Table 2); a category column for ease of relating the specified control back to the area to be protected; and finally implementation guidelines.

Table 2 – Fraud categories and sub-categories

Fraud	Sub-Categories	Definition
Corruption	Conflict of Interest	Where an employee has an undisclosed personal economic interest in a transaction that adversely affects the company.
	Bribery	The offering, giving, receiving or soliciting of anything of value to influence the outcome of a business transaction.
	Illegal Gratuities	Where something of value is given to reward a business decision rather than to influence it.
	Economic Extortion	The demanding of something of value as a condition of awarding business.
Fraudulent Statements	Financial	The deliberate misrepresentation of any item on the company's financial statements.
	Non-Financial	The deliberate misrepresentation of information other than financial, originating either internally or externally.
Asset Misappropriation	Cash – Larceny	Where cash is stolen after it is recorded on the company's books.
	Cash – Fraudulent Disbursements	Where an employee makes a distribution of company funds for a dishonest purpose.
	Cash - Skimming	When cash is stolen before it is recorded in the company's books.
	Non-Cash – Misuse	The use of company assets, other than cash, in a manner other than that intended by the company. Common examples of assets that are misused include vehicles, computers, office equipment, office supplies and information.
	Non-Cash - Larceny	Theft of company assets other than cash. This includes intellectual property which encompasses ideas, designs and innovations whether expressed or recorded.
Destruction of Data		Intentional deletion of company data and/or information.
Social Engineering		Obtaining company information from employees through deceptive means.

3. Guidance for Using the Framework

3.1. Assessment Guidance

As stated in the COSO definition, internal control is a process. This process begins with assessment of the business. The purpose of this assessment is to determine the areas which are most likely vulnerable to fraud, and therefore require intervention to mitigate fraud. The ACFE states that the six highest fraud frequency departments in businesses are accounts, operations, sales, executive/upper management, customer service and purchasing [**2**]. While it is recognized that not all businesses may have all of the departments listed above, the list provides a starting point for assessing fraud risks. Management needs to assess the likelihood of a fraud occurring, the potential significance of the fraud and, should the fraud occur, the likely possible impact. Based on these findings, management should select controls whose costs do not outweigh the benefits of having the control in place.

3.2. Selection Guidance

At its center, this framework has the system or the process that management has determined needs to be safeguarded. Once the system or process has been identified, the next step is to determine which of the three characteristics of information is most critical to the asset. It is possible that more than one may be deemed critical, with no specific characteristic being deemed the most critical.

The characteristic determined to be the most critical to the target system is the third of the circle that will require the most controls. It is recommended that this characteristic should be protected with at least one of each of the administrative, operational and technical control types. Further, the controls selected for this specific characteristic should also consist of preventive and detective controls. Depending on the specific target, it may be desirable to include more than one control in any layer, in order to provide preventative, detective and corrective control. This may be possible without significant costs accruing for the holistic protection of the vulnerable characteristic. Once the critical characteristic has been protected, the other two characteristics should also be protected with at least one control for each third of the circle.

On occasion, more than one characteristic may be deemed as critical. In these instances, it is recommended that each area that is deemed to be critical should be protected at each layer. This will mean that the specific target has more controls over it than others, but this is exactly the reasoning behind making the framework individual and risk-based. The target has more than one critical characteristic and therefore requires more protection than a target with just one critical characteristic.

3.3.Implementation Guidance

The control list provides generic implementation guidance for each possible control. The guidance is intended to provide a general idea of what may be necessary in order to implement the control. Each business and each situation within a business will require different implementation techniques for the same control, and every possible scenario cannot be considered in this list. At the bottom of the implementation guidance section, where appropriate, questions have been provided to assist management in producing a Fraud Risk Assessment and determining whether the specific control is necessary or desirable in their context.

4. Framework Limitations

The framework presented in this paper is intended to give small business owners/managers a basic structure within which to select and implement controls to help in their fight against fraud. The framework has inherent limitations and it makes certain assumptions which are highlighted and discussed below.

The major limitation of the framework is inherent in the fact that it is intended as a guide to assist small businesses in preventing and detecting fraud: fraud is as individual as fraudsters and the environment that the fraud occurs in. However, realistically, fraud, due to its very nature is not entirely preventable. The reality is that an individual intent on perpetrating fraud will find a method to circumvent the most elaborate anti-fraud controls in place. The framework therefore includes controls that can be used to assist in the detection of fraud with the understanding that if you fail to prevent any specific fraud, you should at least have the capacity to detect it before it cripples the business.

Another limitation of the framework is that it assumes that management has intimate knowledge of the business operations and procedures, and that therefore they ought to know which areas of the business are most vulnerable to fraud. While this may be intuitive, and may lead management to implement controls to secure the most easily targeted areas, the successful fraudster may target areas that have been overlooked entirely, or those that have minimum controls implemented. In order to overcome this limitation, all employees of a business should be included in the fraud risk assessment process and should be made aware of common frauds and methods to prevent and detect them.

A further limitation of the framework is grounded in the realities of fraud: it is impossible to measure the effectiveness of the framework. Due to the clandestine nature of fraud, most business owners generally do not know fraud is occurring. However, if the best estimates of the ACFE examiners is to be believed, average business losses are in the range of 5% of annual revenues. While the business owners who decide to use the framework for the effective implementation of controls may see an increase in their annual revenue, there will never be a method of determining whether the controls have minimized the occurrences or the impact of fraud, or whether the business is indeed performing better and the fraudster continues to skim 5% off of the actual revenue.

5. Conclusions and Future Work

The conceptual framework developed in this research is intended to assist small business owners in mitigating occupational fraud in their specific environments. Based on this intention, it was evident that the framework must be customizable to individual circumstances, not only considering business concept, but also taking into account resource constraints such as time, money and expertise. The framework is a threat-based, risk management model, based on the ACFE fraud tree. It is designed as an alternative for smaller enterprises with fewer resources. It can serve as both an internal control framework as well as a template for an internal audit plan. This will encourage small businesses to implement internal controls and maintain an internal audit activity.

The nature of a conceptual framework means that it consciously or unconsciously informs thought and practice, by increasing personal sensitivity to particular occurrences [**11**]. This research draws two distinctly separate concepts familiar to information security practitioners and uses them as the pillars for the development of a fraud risk mitigation framework to assist small business owners in their attempt to mitigate fraud. The two concepts are the CIA triad of information security and defense in depth.

The framework, if used as intended, can assist small business owners in mitigating their occupational fraud risks, even if the results of their mitigation efforts are unquantifiable. The framework, while intended for small business, can produce benefit to business of all sizes. Larger businesses that already have controls in place and functioning can use the graphical representation of the framework in order to verify that their assets and processes are suitably covered. Future research can focus on extending the list of controls for larger business which may be less resource constrained than the target audience of this research. Also, research should be conducted with small business employees both before the use of the framework and post implementation of controls, in order to determine changes to perceived levels of vulnerability of processes and assets within particular businesses.

6. Acknowledgement

"In order to be successful in your research, you must be simultaneously promiscuous, exploitative and adversarial."~ Dr. Dale Lindskog, September 15, 2010

This research would not have been possible without the assistance and guidance of several individuals who in one way or another contributed to the preparation and completion of this paper. First and foremost, my heartfelt gratitude to my academic advisors: Dr. Dale Lindskog, who was always just an email away, and ready to offer inspiration, encouragement and insightful criticisms; Dr. Shaun Aghili for his support, professional guidance and expert advice on matters related to fraud and accounting; Dr. Pavol Zavarsky, for his perpetual enthusiasm to research, his commitment to excellence, and his constant availability in order to ensure the achievement of excellence by his students; and Ron Ruhl, for his patience and support from pre-enrollment to post-graduation.

I would also like to acknowledge faculty member Francis Gichohi for his encouragement, motivation and continued guidance in my career path. This research culminates a period of collaboration with many colleagues, and while I am indebted to all of them, I am especially grateful to David Edwards, Fares Almari and Shafi Alassmi for their friendship, encouragement and inspiration.

I am forever indebted to my family for their unconditional love and support through my course of study, especially to my mother for encouraging me to pursue my dreams, and to Sonia for the interminable moral support given to me. Finally, I would like to thank my son Zachary for accompanying me on my journey. Without his youthful exuberance and sense of adventure, Edmonton would have surely been a lonelier place. – *Fiat Lux*

7. References

[1] Oxford Dictionaries Online. [Online]. http://oxforddictionaries.com/view/entry/m_en_gb0314620#m_en_gb0314620

[2] ACFE, "Report to the Nations," 2010.

[3] SEC. (2008, August) U. S. Securities and Exchange Commission. [Online]. http://www.sec.gov/rules/final/33-8238.htm#iib3a

[4] Coopers & Lybrand, "Internal Control - Integrated framework," Committee of Sponsoring Organizations, 1992.

[5] Committee of Sponsoring Organizations, "Internal Control - Integrated Framework," COSO, 1992.

[6] J. A. Welsh and J. F White, "A Small Business is not a Little Big Business," *Harvard Business Review*, pp. 18-32, 1981.

[7] E. Flamholtz, "Effective Organizational Control: A Framework, Applications, and Implementations," *European Management Journal*, pp. 596-611, 1996.

[8] Brahim Herbane, "Small Business research: Time for a crisis-based view," vol. 28, no. 1, pp. 43-64, February 2010.

[9] Andrew Atherton, "The Uncertainty of Knowing: An Ananlysis of the Nature of Knowledge in a Small Business Context," *Human Relations*, vol. 56, no. 200311, pp. 1379-1398, November 2003.

[10] National Institute of Science and technology, "Guide for Assessing the Security Controls in Federal Information Systems," SP800-53A, 2008.

[11] Mason J. and Waywood A., "The Role of Theory in Mathematics Education and Research," in *International Handbook of Mathematics Education*, Dordrecht, Ed.: Kluwer, 1996, pp. 1055-1089.

APPENDIX 1

Administrative Controls					
Control	Preventive / Detective / Corrective	Confidentiality / Integrity / Availability	Fraud/Threats	Category	Implementation Guidelines
Security Assessment	• Preventive	Confidentiality	• Corruption • Fraudulent Statements • Asset Misappropriation • Destruction of data • Social Engineering	AC	• Determine gaps between where the security is and where management wants it to be • Determine potential threats and select appropriate controls • Prepare Assessment Report including controls
		Integrity	• Corruption – Conflict of Interest • Corruption – Bribery • Corruption – Economic Extortion • Fraudulent Statements • Destruction of Data • Social Engineering	AI	
		Availability	• Asset Misappropriation • Destruction of data • Social Engineering	AA	
Acceptable Use Policy	• Preventive	Confidentiality	• Corruption – Conflict of Interest • Corruption – Bribery • Corruption – Economic Extortion • Fraudulent Statements – Non-Financial • Asset Misappropriation • Social Engineering	AC	• Outline the acceptable usage of the organization's assets, inclusive of its information, information systems, communication equipment, and internet access where applicable. • Include all possible sanctions, or a range of sanctions for unacceptable use • ALL staff, inclusive of management, should acknowledge having read, understood and intention to comply. • Can be "hard copy" paper policy or online policy on a company intranet, signed digitally. Hard copy should be placed in personnel files.
		Integrity	• Corruption – Conflict of Interest • Corruption – Bribery • Corruption – Economic Extortion • Fraudulent Statements • Asset Misappropriation – Cash • Destruction of Data • Social Engineering	AI	

Administrative Controls					
Control	Preventive / Detective / Corrective	Confidentiality / Integrity / Availability	Fraud/Threats	Category	Implementation Guidelines
		Availability	• Corruption – Conflict of Interest • Corruption – Bribery • Asset Misappropriation • Destruction of Data • Social Engineering	AA	*Are there rules or guidelines in place for the use of the business's assets* *Are they communicated to ALL staff and re-circulated periodically?*
Hiring Policy	• Preventive	Confidentiality	• Corruption – Conflict of Interest • Corruption – Bribery • Corruption – Economic Extortion • Fraudulent Statements – Non-Financial • Asset Misappropriation – Non-cash • Social Engineering	AC	• Policy should require the company check references given by prospective employees. • Credit checks should be performed for potential employees. While an unfavorable credit check is not specific reason to not hire an employee, it should be a reason to monitor what the employee has access to within the company. • Integrity check for all potential employees. Past instances of integrity issues are likely to be an indication of future behavior. • Drug testing may be considered depending on the nature of job being offered to the employee. *Do the hiring policies seek out individuals of high moral character?* *Is there screening or testing of employees in trusted or sensitive positions?*
		Integrity	• Corruption – Conflict of Interest • Corruption – Bribery • Corruption – Illegal gratuities • Fraudulent Statements • Asset Misappropriation – Cash • Destruction of Data • Social Engineering	AI	

Administrative Controls					
Control	Preventive / Detective / Corrective	Confidentiality / Integrity / Availability	Fraud/Threats	Category	Implementation Guidelines
User Installed Software	• Preventive	Integrity	• Fraudulent Statements • Destruction of Data • Social Engineering	AI	• Users should be restricted from installing software. • Users who must have administrative privileges on their machines in order to perform their jobs, should sign a policy document stating that they will not install software on their machines. • Software should be checked by competent individuals to ensure that it is permissible before installation. • Software installed on company machines must be licensed to the company, as the company will be held liable for pirated software found on their machines. • Unknown software may lead to unnecessary vulnerabilities in the company network, which may be unknown until too late. *Are machines audited periodically to ensure that there is no unlicensed software installed?* *Is there a process in place to renew software licenses upon expiry?* *Are all employees aware of the consequences to individuals and businesses, of software piracy?*
		Availability	• Asset Misappropriation • Destruction of Data • Social Engineering	AA	
Mandatory Vacation	• Preventive • Detective	Integrity	• Corruption • Fraudulent Statements • Asset Misappropriation	AI	• All employees should be made to take annual vacation leave, either at the time it is due to them, or at a time when it is

Administrative Controls					
Control	Preventive / Detective / Corrective	Confidentiality / Integrity / Availability	Fraud/Threats	Category	Implementation Guidelines
			• Destruction of Data • Social Engineering		convenient to the company. • Annual vacation leave should not necessarily be at the same time every year, and employees should be flexible about when they take leave. An employee who demands annual leave at a certain period, and is totally inflexible may be committing a fraud against the company. • Employees in sensitive positions should be made to take leave long enough to require someone else to perform their duties for a full cycle. Eg. Accounting employees should be on leave for the monthly closing of the books; payroll employees should be on leave when the payroll is actually run. *Are annual vacations mandatory for all staff?*
Job Rotation	• Preventive • Detective	Integrity	• Corruption • Fraudulent Statements • Asset Misappropriation • Destruction of Data • Social Engineering	AI	• Employees are rotated to different areas of the company to perform different jobs. • Allows for the educating employees in various areas of operations and minimizes impact of non-availability of any specific employee • Precautions should be taken to ensure that least privilege is maintained over time. This means that employee's logical and physical access needs to be changed each time the employee

Administrative Controls					
Control	Preventive / Detective / Corrective	Confidentiality / Integrity / Availability	Fraud/Threats	Category	Implementation Guidelines
					changes job function. • One downside of this control is that employees now have knowledge of more organizational processes and is better equipped to commit fraud.

Operational Controls					
Control	Preventive / Detective / Corrective	Confidentiality / Integrity / Availability	Fraud/Threats	Category	Implementation Guidelines
Security Awareness and Training	• Preventive • Detective	Confidentiality	• Corruption – Conflict of Interest • Corruption – Bribery • Fraudulent Statements – Non-Financial • Asset Misappropriation – Non-Cash • Destruction of Data • Social Engineering	OC	• Develop a training policy that will define purpose, roles, level of training required. • Ensure all staff are aware of policy. • Require all users to receive training. • Require users to sign off on having read, understood, and intending to comply with policy, before access to organizational information and systems is provided. • Require all staff to receive training as appropriate, but within a specified maximum timeframe. • Select appropriate awareness and training topics relevant to the organizational objectives and procedures. • Select appropriate methods of delivering awareness and training, based on size of organization and available resources. • Maintain records detailing which staff members attended which sessions. *Does the business exhibit fraud awareness?* *Do supervisors, management AND the Board of Directors receive fraud awareness training?* *Do ALL employees receive security training?* *Is there a policy against employees allowing physical and/or logical access to unauthorized personnel?* *Do any employees exhibit a change in behavior?*
		Integrity	• Corruption • Fraudulent Statements • Asset Misappropriation – Cash • Asset Misappropriation – Non-Cash – Misuse • Destruction of Data • Social Engineering	OI	
		Availability	• Asset Misappropriation • Destruction of Data • Social Engineering	OA	

Operational Controls					
Control	Preventive / Detective / Corrective	Confidentiality / Integrity / Availability	Fraud/Threats	Category	Implementation Guidelines
Segregation of Duties	• Preventive	Integrity	• Corruption • Fraudulent Statements • Asset Misappropriation – Cash • Destruction of Data • Social Engineering	OI	• No employee should have exclusive control over any transaction or group of transactions from beginning to end. • If human resource constraints dictate, at-risk transactions should be passed between differing individuals in such a manner that the same individual is not responsible for critical aspects of the transaction. • Where separation of duty is not possible, other controls should be in place such as audit trail, reconciliation, exception reports or management review. *Is there a policy that restricts access to ONLY those requiring it specifically for the performance of their job?* *Are incompatible duties segregated/separated?* *Are duties divided so that no single employee acting alone, controls all phases of a transaction?*
		Availability	• Asset Misappropriation – Cash • Destruction of Data • Social Engineering	OA	
Background Investigation	• Preventive	Confidentiality	• Corruption – Conflict of Interest • Corruption – Bribery • Corruption – Illegal gratuities • Fraudulent Statements • Asset Misappropriation • Destruction of Data • Social Engineering	OC	• All potential candidates for positions of trust should provide authorization to the business to conduct background checks on them. The business should absolutely use this authority when the potential candidates will have access to sensitive assets. • Background checks may reveal

Operational Controls					
Control	Preventive / Detective / Corrective	Confidentiality / Integrity / Availability	Fraud/Threats	Category	Implementation Guidelines
		Integrity	• Corruption – Conflict of Interest • Corruption – Bribery • Corruption – Illegal gratuities • Fraudulent Statements • Asset Misappropriation – Cash • Destruction of Data • Social Engineering	OI	something in an individual's past that someone else may use to bribe the individual into committing fraud against the business. • If a current employee is considered for a promotion into a position of trust, the same authorization should be provided as that required for new employees. • Non-routine background checks should be performed if an employee begins to exhibit unusual behavior. *Do employees in positions of trust sign authorizations for the business to conduct full background investigations on them at any time while employed by the business in a position of trust?*
Security Audits	• Preventive • Detective	Confidentiality	• Corruption • Fraudulent Statements • Asset Misappropriation • Destruction of Data • Social Engineering	OC	• Intended to test compliance with the policies of the business and will therefore be based on the policies established. • All employees should be communicated with during a security audit. This can be done by casual conversation and/or by observing how they conduct themselves during the course of their business day. • In order to be effective, security audits should be unscheduled. • Work areas should be checked for written passwords, confidential information left on desks, or not correctly disposed of.
		Integrity	• Corruption • Fraudulent Statements • Asset Misappropriation – Cash • Destruction of Data • Social Engineering	OI	
		Availability	• Corruption – Conflict of Interest • Corruption – Bribery • Corruption – Illegal gratuities • Fraudulent Statements	OA	

Operational Controls					
Control	Preventive / Detective / Corrective	Confidentiality / Integrity / Availability	Fraud/Threats	Category	Implementation Guidelines
			• Asset Misappropriation – Cash • Destruction of Data • Social Engineering		*Have there been previous security audits?* *Have past compliance breaches been remediated?* *Have the policies changed since the last audit?* *Have the policies changed since the last attempted or successful fraud?* *Are there any new employees who have not signed their intention to comply with the security policy of the business?*
Authorization Limits	• Preventive	Integrity	• Corruption - Bribery • Fraudulent Statements • Asset Misappropriation - Cash	OI	• Establish limits for all employees who are in a position to obligate the business to external third parties. • Limits should also be placed on the posting of financial transactions that may not involve external third parties. *Do supervisors review and sign-off on subordinates work?*
Reconciliations	• Detective	Integrity	• Fraudulent Statements • Asset Misappropriation - Cash	OI	• Monthly reconciliations should be performed on accounts payable, accounts receivable and bank statements. • Variances should be investigated immediately and remediated as necessary. • Reconciliations should be signed by the person performing them and based on seniority level, may require signature by a senior employee after review. *Are bank accounts reconciled monthly?*

Operational Controls					
Control	Preventive / Detective / Corrective	Confidentiality / Integrity / Availability	Fraud/Threats	Category	Implementation Guidelines
					Are supplier Accounts Payable (AP) statements reconciled monthly? *Are Accounts Receivable (AR) accounts reconciled monthly?* *Is a monthly or annual variance analysis performed?*
Physical Security	• Preventive • Detective	Confidentiality	• Corruption – Bribery • Fraudulent Statements • Asset Misappropriation • Destruction of Data • Social Engineering	OC	• Need not be computerized or highly technical. • Locks should be placed on all internal and external doors which allow access to sensitive data. These areas include server rooms, and finance areas. Production areas can also be included if proprietary information could be accessed by unauthorized presence in the area. • Access to these areas should be restricted to individuals with a legitimate business need to perform their duties. • Whatever method is used to grant access should afford an opportunity for logging the time and the individuals that enter and exit. • Surveillance cameras can be utilized inside of these areas and where they are used they should have the capacity to record and store footage. *Is there electronic surveillance?* *Is there a policy of locking doors, desks*
		Integrity	• Corruption – Conflict of Interest • Corruption – Bribery • Fraudulent Statements • Asset Misappropriation • Destruction of Data • Social Engineering	OI	
		Availability	• Corruption – Conflict of Interest • Corruption – Bribery • Corruption – Illegal gratuities • Fraudulent Statements • Asset Misappropriation • Destruction of Data • Social Engineering	OA	

Operational Controls					
Control	Preventive / Detective / Corrective	Confidentiality / Integrity / Availability	Fraud/Threats	Category	Implementation Guidelines
					and/or filing cabinets?
Periodic Audits	• Preventive • Detective	Integrity	• Fraudulent Statements • Asset Misappropriation • Destruction of Data • Social Engineering	OI	• Audits should be scheduled periodically during the year, and conducted as scheduled. • Audits can be conducted by supervisors, managers or external third parties. *Is there an internal audit activity?*
Surprise Audits	• Preventive • Detective	Integrity	• Fraudulent Statements • Asset Misappropriation • Destruction of Data • Social Engineering	OI	• Audits which are unscheduled should be performed, even if scheduled audits are conducted on a regular schedule. • The possibility of unscheduled periodic audits has the potential to influence daily behavior because employees always know that there is a risk of being audited. • These audits can be conducted by supervisors, managers or external parties. *Does the company have assets that are easily convertible and physically available to employees?* *Is there an internal audit function?*
External Audits	• Preventive	Integrity	• Fraudulent Statements • Asset Misappropriation • Destruction of Data • Social Engineering	OI	• Auditors should be selected based on the scope of the audit and familiarity with the specific industry. • External audits can be financial or systems audits, or a combination. • Required for external financing, and should be performed even when

Operational Controls					
Control	Preventive / Detective / Corrective	Confidentiality / Integrity / Availability	Fraud/Threats	Category	Implementation Guidelines
					external financing is not required. • External parties have none of the prejudices that internal entities may have, and therefore may be more capable of spotting irregularities. *Are external audits performed on a regularly scheduled basis?* *Does the external audit cover both financial and Information Technology?*
Disaster Plan	• Preventive • Corrective	Availability	• Asset Misappropriation • Destruction of Data • Social Engineering	OA	• Disasters can be natural or man-made and a business should prepare for both types. • The effects are generally spread further and last longer than an emergency and therefore the plan should include response and recovery. • Recovery may be necessary at an alternate location either short or long term. *Is the business aware of the potential types of disasters for their geographic location?* *Has the business taken into consideration the possibility of man-made disasters?*
Emergency Plan	• Preventive • Corrective	Availability	• Asset Misappropriation • Destruction of Data • Social Engineering	OA	• In an emergency, the human assets are the most important assets to safeguard. • Assets critical to the survival of the business should be protected if/when possible. • Once the emergency is over, you may need to revert to a Disaster Plan.

Operational Controls					
Control	Preventive / Detective / Corrective	Confidentiality / Integrity / Availability	Fraud/Threats	Category	Implementation Guidelines
					Does the business have an emergency plan to ensure the safety of human assets?
Contingency Plan	• Preventive • Corrective	Availability	• Asset Misappropriation • Destruction of Data • Social Engineering	OA	• Contingency plans can form the basis of the disaster and the emergency plan. They tend to be more event specific than the two previously mentioned plans. • The underlying purpose of a contingency plan is to keep the business in operation regardless of the type of event threatening disruption. • The plans should provide specific tasks that should be performed in the case of each event covered. • The plan should be communicated to the relevant parties and maintained in a current state based on organizational resources and processes. *Does the business have a plan to deal with the impact of the unanticipated departure of a key employee?*
Information System Backup	• Corrective	Integrity	• Fraudulent Statements • Asset Misappropriation – Cash • Destruction of Data • Social Engineering	OI	• Backup user and system information on a regular schedule determined by how often changes are made to the system and the criticality of the system to the organization's objectives. • Backups should be stored offsite. • Backups could be encrypted if confidentiality is a requirement.
		Availability	• Asset Misappropriation • Destruction of Data • Social Engineering	OA	

Operational Controls					
Control	Preventive / Detective / Corrective	Confidentiality / Integrity / Availability	Fraud/Threats	Category	Implementation Guidelines
					• Backups should be protected while in transit to the offsite location. *Has the business ever attempted to restore data from a backup location or device?* *Has the manager or a trusted employee inspected the offsite backup location for geographic suitability, and storage conditions?*

Technical Controls

Control	Preventive / Detective / Corrective	Confidentiality / Integrity / Availability	Fraud/Threats	Category	Implementation Guidelines
Access Control	• Preventive	Confidentiality	• Fraudulent Statements – Non-Financial • Asset Misappropriation – Non-Cash • Social Engineering •	TC	• Access control may begin with a formal written policy that is then implemented in the software of the information system. • First determine access needed by each staff member to perform their job. • Determine if groups are possible based on requirements. • If using groups, divide staff members into relevant groups (eg. By department) • Create specific access control policies and groups if necessary, in the operating system, and assign each member to their group, or give access to only what they need to perform their job functions. *Are there adequate physical access controls?* *Is there a policy that restricts access to ONLY those requiring it for job performance?* *Is there a policy against employees allowing access to unauthorized personnel?*
		Integrity	• Fraudulent Statements • Asset Misappropriation – Cash • Destruction of Data • Social Engineering	TI	
		Availability	• Asset Misappropriation • Destruction of Data • Social Engineering	TA	
Identification	• Preventive	Confidentiality	• Fraudulent Statements – Non-Financial • Asset Misappropriation – Non-Cash • Social Engineerings	TC	• Provide each authorized user with a system identifier based on the naming standard (eg. lastname.first name)

Technical Controls					
Control	Preventive / Detective / Corrective	Confidentiality / Integrity / Availability	Fraud/Threats	Category	Implementation Guidelines
		Integrity	• Fraudulent Statements • Asset Misappropriation – Cash • Destruction of Data • Social Engineering	TI	• Each system must be configured to require a user to identify themselves before access is granted. *Does the organization use ID's and passwords?* *Are there strict requirements for the use of complex passwords?* *Is there a password policy requiring a password change at least every 90 days?*
		Availability	• Asset Misappropriation • Destruction of Data • Social Engineering	TA	
Authentication	• Preventive	Confidentiality	• Fraudulent Statements – Non-Financial • Asset Misappropriation – Non-Cash • Social Engineering	TC	• Following the identification of a user, the system needs to be able to authenticate the user. • Authentication is commonly provided by a password. • Organization should have a password policy stating minimum password length, maximum allowed time between password change, password complexity requirements. *Are there strict requirements for the use of complex passwords?* *Is there a password policy requiring a password change at least every 90 days?*
		Integrity	• Fraudulent Statements • Asset Misappropriation • Destruction of data • Social Engineering	TI	
		Availability	• Asset Misappropriation • Destruction of Data • Social Engineering	TA	
Account Management	• Preventive	Confidentiality	• Fraudulent Statements – Non-Financial • Asset Misappropriation – Non-Cash • Destruction of Data • Social Engineering	TC	• Determine account types needed (eg. Individual, group, administrator). • Determine requirements for each account, and authorization associated

Technical Controls					
Control	Preventive / Detective / Corrective	Confidentiality / Integrity / Availability	Fraud/Threats	Category	Implementation Guidelines
		Integrity	• Fraudulent Statements • Asset Misappropriation • Destruction of Data • Social Engineering	TI	with account types, as well as naming standard (eg. lastname.first name) • Confirm authorized users and associated privileges. • Review and modify as organizational changes occur. • Temporary employees should be given limited access and accounts should be time-limited to the expiration of their employment period. • Delete accounts as individuals leave organization.
		Availability	• Asset Misappropriation • Destruction of Data • Social Engineering	TA	
Least Privilege	• Preventive	Confidentiality	• Corruption – Conflict of Interest • Corruption – Bribery • Fraudulent Statements • Asset Misappropriation – Cash • Destruction of data • Social Engineering	TC	• Users are given only the privileges they need in order to perform their jobs. • Based on users' job tasks, they are restricted to only the parts of system they need to perform their jobs. • Only applications needed are accessible on their machines, and in these applications they can only perform tasks necessary for them to do their jobs. *Is there a policy that restricts access to ONLY those requiring it for job performance?*
		Integrity	• Corruption – Conflict of Interest • Corruption – Bribery • Fraudulent Statements • Asset Misappropriation – Cash • Destruction of Data • Social Engineering	TI	
Session Lock	• Preventive	Confidentiality	• Fraudulent Statements – Non-Financial • Asset Misappropriation – Non-Cash • Social Engineering	TC	• The system is set to lock the session of all users after a specified amount of time of inactivity on the account.

Technical Controls					
Control	Preventive / Detective / Corrective	Confidentiality / Integrity / Availability	Fraud/Threats	Category	Implementation Guidelines
		Integrity	• Fraudulent Statements • Asset Misappropriation – Cash – Larceny • Asset Misappropriation – Cash – Fraudulent Disbursements • Asset Misappropriation – Non-Cash • Destruction of Data • Social Engineering	TI	• In order to unlock the session, the user must supply the credentials again. • The accounts should also be set so that users can lock their sessions if they will be temporarily away from their systems. *Are users trained to lock their systems with ctrl-alt-del every time they move from their systems?*
		Availability	• Asset Misappropriation – Cash – Larceny • Asset Misappropriation – Cash – Fraudulent Disbursements • Asset Misappropriation – Non-cash • Destruction of Data • Social Engineering	TA	
Session Termination	• Preventive	Confidentiality	• Fraudulent Statements – Non-Financial • Asset Misappropriation – Non-cash • Social Engineering	TC	• The system automatically terminates a session after a specified period of inactivity. • In order to reestablish a session after termination, the user must initiate a new connection to the system. • Can apply to local and remote sessions.
		Integrity	• Fraudulent Statements • Asset Misappropriation – Cash – Larceny • Asset Misappropriation – Cash – Fraudulent Disbursements • Asset Misappropriation – Non-Cash • Destruction of Data • Social Engineering	TI	

Technical Controls					
Control	Preventive / Detective / Corrective	Confidentiality / Integrity / Availability	Fraud/Threats	Category	Implementation Guidelines
		Availability	• Asset Misappropriation – Cash – Larceny • Asset Misappropriation – Cash – Fraudulent Disbursements • Asset Misappropriation – Non-cash • Destruction of Data • Social Engineering	TA	
Unsuccessful Login Attempts	• Preventive	Confidentiality	• Fraudulent Statements – Non-Financial • Asset Misappropriation – Non-Cash • Social Engineering	TC	• The system is set to enforce a limit on the maximum number of incorrect login attempts by users during a specified time period. Once this limit is reached, the system automatically locks the account. • Based on the number of users, the lockout can be set to be released after a certain time period, or by a System Administrator. *Is there a minimum time limit set before a user can attempt to sign in after lockout? Can the administrator override the lockout?*
		Integrity	• Fraudulent Statements • Asset Misappropriation – Cash – Larceny • Asset Misappropriation – Cash – Fraudulent Disbursements • Destruction of Data • Social Engineering	TI	
		Availability	• Fraudulent Statements • Asset Misappropriation – Cash – Larceny • Asset Misappropriation – Cash – Fraudulent Disbursements • Destruction of Data • Social Engineering	TA	
Patch Management	• Corrective	Confidentiality	• Fraudulent Statements – Non-Financial • Asset Misappropriation – Non-Cash • Social Engineering	TC	• Company must ensure that software vendor released security related patches are installed in a timely manner on all

Technical Controls					
Control	Preventive / Detective / Corrective	Confidentiality / Integrity / Availability	Fraud/Threats	Category	Implementation Guidelines
		Integrity	• Fraudulent Statements • Asset Misappropriation • Destruction of Data • Social Engineering	TI	systems running the specified software. • Patch should be tested on a single non-critical machine if possible, prior to installation on all systems. • Service packs and hot fixes should also be treated in a similar manner. *Does the business have a patch management policy?* *Are all systems configured identically, and carrying the same software versions?*
		Availability	• Asset Misappropriation • Destruction of Data • Social Engineering	TA	
Firewall	• Preventive	Integrity	• Fraudulent Statements • Asset Misappropriation – Non-Cash • Destruction of Data • Social Engineering	TI	• Network based and host based firewalls should be installed and functional. • Firewalls should be configured to inspect both incoming and outgoing packets, from internal and external sources. • A trusted insider with remote access could maliciously insert a rogue packet while outside the organization, just as easily as from inside the organization's perimeter. • Organizational networks should be configured in such a manner to ensure that if a network based firewall is breached, that all internal hosts are not automatically vulnerable. *Has the business segmented its network based on access requirements?* *Are business-critical servers on a different network segment available to internal hosts only?*
		Availability	• Fraudulent Statements • Asset Misappropriation – Non-Cash • Destruction of Data • Social Engineering	TA	

Technical Controls					
Control	Preventive / Detective / Corrective	Confidentiality / Integrity / Availability	Fraud/Threats	Category	Implementation Guidelines
Anti-virus Software	• Preventive • Detective	Confidentiality	• Corruption – Economic Extortion • Fraudulent Statements • Asset Misappropriation – Non-Cash • Destruction of Data • Social Engineering	TC	• Anti-virus software should be installed on all computer systems within the organization. • Any third party systems that are allowed to be connected to the system should also be checked to confirm that they have anti-virus software running. • Anti-virus software needs to be updated as often as possible and shoul therefore be configured to scan for updates and install them without requiring user intervention. • This update installation should be run in the background unknown to users of the systems. The update settings should be subject to organizational policy and should be unchangeable by employees, except a designated system administrator. *Are all business machines configured to automatically update anti-virus software in the background?*
		Integrity	• Corruption – Economic Extortion • Fraudulent Statements • Asset Misappropriation – Non-Cash • Destruction of Data • Social Engineering	TI	
		Availability	• Corruption – Economic Extortion • Fraudulent Statements • Asset Misappropriation – Non-Cash • Destruction of Data • Social Engineering	TA	
Encryption	• Preventive	Confidentiality	• Asset Misappropriation – Non-Cash • Destruction of Data • Social Engineering	TC	• All organizational data does not necessarily require encryption. • Data that may be remotely accessible to

Technical Controls					
Control	Preventive / Detective / Corrective	Confidentiality / Integrity / Availability	Fraud/Threats	Category	Implementation Guidelines
		Integrity	• Fraudulent Statements • Asset Misappropriation – Non-Cash • Destruction of Data • Social Engineering	TI	trusted individuals over an untrusted network should be considered as candidates for encryption. • Sensitive information should be encrypted at all stages of its life, even if it is not remotely accessed. • The encryption method(s) chosen for particular uses should be cost effective based on the value of the data being secured. • Hash values can be used to perform Integrity checks.
Audit Trail/Log	• Preventive • Detective	Integrity	• Fraudulent Statements • Asset Misappropriation – Cash • Asset Misappropriation – Non-Cash • Destruction of Data • Social Engineering	TI	• Used to prevent and detect unauthorized activities. • At a minimum, the system should be configured to log: o individual access to the system, inclusive of date and time, o Files accessed o Files attempted to be accessed but denied. o Unauthorized access attempts, date and time. • Based on the potential evidentiary value of audit logs, they should be stored in a secured folder, and be accessible by only a few select trusted individuals.
		Availability	• Fraudulent Statements • Asset Misappropriation – Cash • Asset Misappropriation – Non-Cash • Destruction of Data • Social Engineering	TA	

Technical Controls					
Control	Preventive / Detective / Corrective	Confidentiality / Integrity / Availability	Fraud/Threats	Category	Implementation Guidelines
Exception Reports	• Detective	Confidentiality Integrity	• Fraudulent Statements • Asset Misappropriation – Cash – Fraudulent Disbursements • Asset Misappropriation – Non-Cash • Destruction of Data • Social Engineering	TE	• Systems should be configured to report activity that is outside of the expected parameters - This activity will vary from system to system. • Exception reports must be monitored by a senior member of the business. • Exceptions must be investigated and cleared to determine both the cause and the effect. Where necessary remedial action should be taken immediately. Are exception reports stored in a secured place? (Both hard copy and soft copy)
Wireless Access Restrictions	• Preventive	Confidentiality	• Fraudulent Statements – Non-Financial • Asset Misappropriation – Non-Cash • Social Engineering		• Establish wireless usage restrictions. • Configure wireless access points to require authentication. • Wireless access points should be positioned to cover the organizational perimeter, but not to extend beyond it. • Give authorized users wireless access.
		Integrity	• Fraudulent Statements • Asset Misappropriation – Cash • Destruction of Data • Social Engineering		
		Availability	• Asset Misappropriation • Destruction of Data • Social Engineering		