Vol. 01, No. 03: July (2016)

Journal of Business

Open access available at http://journalofbusiness.us

JOURNAL OF BUSINESS

Fraud, security, and Controls in Small Businesses: A Proposed Research Agenda

Robert Stone[a*]

[a] University of Idaho.
[*]Corresponding author's email address: rstone@uidaho.edu.

ARTICLE INFO

Received: 03-06-2016
Accepted: 09-07-2016
Available online: 12-07-2016

Keywords:
Fraud; Internal Controls; Small Business Management

JEL Classification: M10; M40; M41.

ABSTRACT

Fraud and security issues are significant problems faced by businesses. Based on a survey of certified fraud examiners reported in the 2016 ACFE Report to the Nations, total annual loses of all businesses exceeded six billion dollars with an average per case loss just under three million dollars. Small businesses, defined as those with less than 100 employees, reported median fraud losses that were virtually identical to the losses of large businesses. However, given the relative magnitude of assets for these two sizes of businesses, the fraud losses for small businesses have a much bigger impact on small businesses than on large ones. Given the importance of fraud loses to small businesses, fraud, security, and compliance issues are discussed within this context at a conceptual level along with a proposed research agenda.The presented discussion is framed within the special problems, issues, and potential solutions to fraud and compliance in small businesses. We begin with security and compliance issues faced by all businesses. The essence is that the security and compliance solutions (e.g., software) suitable for large businesses are often inappropriate for small businesses. Based on these results, recommendations for small business controls are offered. After discussing the need to perform additional research in this area, a research agenda is proposed. The specific topics of identifying the target population, methods of fully understanding the target population, data collection and analysis, and potential manuscripts are presented. A brief summary of the paper is then provided.

DOI: http://dx.doi.org/10.18533/job.v1i6.44 | ISSN: 2380-4041 (Print), 2380-405X (Online)

1.0 Introduction

Fraud and security issues are continuing problems faced by businesses. A study based on a survey of certified fraud examiners confirms the importance of these issues ("2016 ACFE Report to the Nations," 2016). From cases reported by certified fraud examiners responding to the survey, total losses of $6.3 billion were identified across all organizations. The average loss per case was $2.7 million with a median loss of $150,000 per case. Among these cases 23.2% had losses of $1 million or more. From this same report the most common form of fraud was asset misappropriation (e.g., billing schemes, check tampering) at 83% of all cases with a median loss of $125,000. The least common type of fraud reported was financial statement misrepresentation at less than 10% of the cases but with a median loss of $975,000.

The median length of the reported frauds was 18 months and it was shown that the magnitude of a fraud's loss was positively correlated with its length. The methods by which these frauds were detected were also reported in the survey results ("2016 ACFE Report to the Nations," 2016). In 94.5% of the reported fraud cases, the perpetrator took efforts to conceal their fraud. Most commonly their concealment was done by altering documents. The most common detection method was a tip line at 39.1%. The availability of a telephone hotline encouraged these tips and to a lesser extent the ability to provide tips via email or web-based forms. Whistleblowers also provided detection in some of the reported fraud cases. Among these whistleblowers almost 21% reported their concerns to their direct supervisor while 18% reported to a company executive.

While the above statistics are reported for all the organizations, for the focus here we turn to fraud in small businesses. Much of the attention regarding fraud reported in the popular press has examined fraud in large organizations, yet small businesses face their own distinct, unique fraud threats (Jackson, Holland, Albrecht, and Woolstenhulme, 2010; Laufer, 2011). There are a variety of definitions for small verses large businesses. In this study and as reported in the 2016 ACFE Report to the Nations a business is defined as small if it employs less than 100 employees and large if it has 10,000 employees or more. For both sizes of organizations the median losses from fraud were virtually identical. However, given the relative magnitude of assets for these organizations, the fraud losses for small businesses have a much bigger impact on small businesses relative to large ones. The typical form of fraud differs between these two groups as well. Check tampering, skimming, payroll, cash larceny were reported twice as frequently in small businesses then in large businesses. Internal controls designed to prevent and detect fraud also differ between large and small businesses. The survey results indicate that small businesses implement internal controls at a much lower rate than large businesses. This gap in control implementation leaves small businesses susceptible to fraud and damage to their relatively limited financial resources.

The purpose of the above discussion is to illustrate the occurrence of fraud in businesses and the differences in fraud between small and large businesses as well as the internal controls implemented by these businesses. The fundamental idea is to illustrate that small businesses face different types and occurrence rates of fraud as well as different internal controls implemented by these businesses. These unique issues faced by small businesses provide the focus for this manuscript. This focus is, for small businesses, which frauds are faced, which controls are implemented, and how effective these controls are. Within this context a research agenda is proposed to explore these issues in greater detail.

Our discussion begins with an overview of the fraud, security, and compliance issues specifically experienced by small businesses. Included in this discussion are the constraints faced by small businesses. This is followed by a presentation of recommendations for small business controls. Within these recommendations, presentations are made about the control environment and internal controls for small businesses. The development and effectiveness of these controls are discussed followed by a discussion of small business security and compliance software. The manuscript concludes with recommendations for a research agenda examining these small business issues in greater detail and a brief summary.

2.0 Small businesses and security and compliance issues

Small businesses are natural targets for thrift and fraud ("Effective Internal Control for Small Medium Business"). As mentioned earlier, small businesses typically lack the resources, expertise, and experience to successfully implement security and control systems and often experience time pressures leaving little time for planning (Dawson, 2015; Spencer, n.d.). Failed control systems frequently lead to asset loses, fraud, inefficiency and waste, mismanagement, loss of consumer confidence, and failure to reach business objectives ("Internal Controls-Keys to Business Success").

Internal controls are policies, processes, or procedures within the accounting cycles designed to prevent, detect, or correct errors and fraud (Turner and Weickgenannt, 2013). There are a variety of categorizations for internal controls. One such categorization groups these controls as authorization, adequate documentation, physical security, segregation of duties, and independent reconciliation (Turner and Weickgenannt, 2013). Small and large businesses face different challenges and opportunities when implementing internal controls. In general, small businesses have less formalized structures and procedures operationalizing and facilitating these internal controls than do large businesses. Within this context, the informality of small businesses can weaken authorization internal controls by not requiring a specific manager or employee to authorize certain types of transactions. Similarly, small business informality may not encourage the generation and storage of documentation adequate to allow the recreation of transaction details and as a result produce weak adequate documentation internal controls. Small businesses also frequently have weak physical security internal controls due to this informality. Key business documents (e.g., purchase orders, invoices, and checks) and access to the accounting information system may be available to employees and individuals who do not have a true business need for these documents and access.

By the definition of a small business that is used here, a small business has fewer employees than do large businesses. The limited number of employees influences a small business' ability to implement two other categories of internal controls, segregation of duties and independent reconciliation. A strong segregation of duties control divides three key steps in processing a transaction, authorization, recording, and custody of the resulting assets, across three different employees. In this way, three employees must collude in order for fraud to occur. Small businesses tend to have weak segregation of duties controls due to an insufficient number of employees to allow such segregation. Large businesses typically do not face this same constraint. Similarly, independent reconciliation controls in small businesses tend to be weak. An independent reconciliation requires an individual not involved in the transactions to review them for errors and fraud. Due to the limited number of employees in a small business, it is difficult to find an appropriate individual not involved in these transactions to perform a reconciliation. Someone outside the business could be hired to perform this reconciliation (e.g., CPA), however this places an additional strain on the limited resources of a small business.

Businesses implement security and control systems for a variety of reasons, including demands from regulators and trading parties (Hibbert, 2012). In response to these demands, businesses are often expected to purchase and implement specific security and compliance software regardless of organizational size or complexity. The implementation of such security and compliance solutions in a one size-fits-all manner can actually make these business systems less secure (Hibbert, 2012). The primary reasons are rooted in the characteristic of the implementing business. Small businesses often lack the time, resources, and in-house skills and resources to successfully implement, maintain, and use such software (Hibbert, 2012). One potential solution is to implement an automated accounting system such as Microsoft Small Business Accounting and make use of the security and compliance controls within this software (Spencer, n.d.). These software packages provide some degree of accounting controls to safeguard assets and provide reliability of financial records (Spencer, n.d.). Examples of these controls include general controls providing access security and backup procedures and application controls for input processing, and output in specific accounting modules or cycles.

Attempting to generalize from these observations, one can see that the control environment, or the context in which a business must implement its controls, is critical. There are a variety of characteristics shaping the control environment. Examples of these characteristics include industry, location, and organizational size and type. All influence the businesses' goals, objectives, operations, and activities. The types and complexity of appropriate controls for a specific business depend on its characteristics ("Internal Controls-Keys to Business Success"). Thus, the control environment influences the type and complexity of appropriate accounting controls for the business ("Internal Controls-Keys to Business Success"). In addition to the general and application controls mentioned above, businesses may also effectively use administrative controls to help define their control environment and simultaneously promote operational efficiency (Spencer, n.d.). Examples of administrative controls include written codes of conduct, recruitment and hiring practices, and documented organizational structure (Spencer, n.d.). It would be unrealistic to expect many small businesses to have many administrative controls (Spencer, n.d.).

3.0 Recommendations for small business control

Based upon the above discussion, some recommendation for small businesses seeking to improve control and their control systems can be offered. These recommendations are organized into three broad groups, understanding the small business control environment, developing internal controls, and security and compliance software for small businesses.

3.1 Understanding the small business control environment

The first step is for the owner or senior management of the small business to understand the environment for controls unique to the business ("Effective Internal Control for Small Medium Business"; "Internal Controls-Keys to Business Success"). In specific terms, first identify high risk fraud areas. These are commonly cash receipts and disbursements, receivables, and inventory. Within these high risk areas define business objectives and structures ("Internal Controls-Keys to Business Success") such as maximum error amounts or rates, maximum cycle times, and reconciliation intervals. Within this defined context, controls can be developed addressing the identified, potential threats (Spencer, n.d.).

3.2 Developing internal controls

At a general level, there are three principles for developing internal controls for small businesses. First, it is important to focus on building redundancy into these controls (Hess and Contrell, 2016). Second, it is critically important to address the segregation of duties, which is particularly difficult in a small businesses due to a limited number of organizational employees. Potential solutions to segregation of duties issues could be found in employees sharing key duties or jobs ("Effective Internal Control for Small Medium Business"). Such sharing can be accomplished by training multiple employees to perform the same key job tasks and then staggering their schedule to perform these tasks ("Effective Internal Control for Small Medium Business"). Notice that collusion would be needed among these employees for undetected fraud to occur for long. Finally, the owner and senior managers should monitor the lifestyles of their key employees for indications of incentives to commit fraud ("Effective Internal Control for Small Medium Business").

Several specific internal controls include limiting who can sign business checks as well as who has access to blank documents, including checks. Similarly, limiting the individuals who can approve invoices and purchase orders and not to allow the same employee to both approve invoices and to sign checks. Furthermore, make sure different employees approve and process cash receipts and cash disbursements. Assure that bank statements, cancelled checks and credit card statements are sent to a third party (e.g., external CPA) or a non-work address. Finally, before hiring potential employees, perform meaningful background checks, particularly focusing on past theft and any personal financial pressures ("8 Simple Internal Controls for Small Businesses", 2008).

3.3 Security and compliance software for small businesses

As mentioned earlier, one control approach used by small businesses is to purchase commercial software to facilitate the accounting functions and provide security and compliance and as a result internal controls. There are some suggestions for selecting such software. The hope is that these suggestions can facilitate small business adoption and effective use of this software thereby improving security, compliance, and internal control. First, select software that consolidates functionality so there is one consistent interface. Second, make sure the system allows owners and managers data to focus on actions prioritized by risk. Third, select software allowing process automation so users can focus their attention on high priority areas rather than routine tasks. This also helps reduce end-user errors. Fourth, the software system should provide senior managers feedback on business performance to assess security and compliance effectiveness. Fifth, it is best if the selected software can be implemented in a phased manner allowing owners and senior management to select modules to gradually implement into the business so as to avoid overwhelming employees. Finally, an ability to select and/or simplify security features to address specific security risks is desirable (Hibbert, 2012).

4.0 The Method

The approach or method of this research is to use literature and conceptual arguments to organize a discussion of small business fraud, security, and controls. Part of this discussion includes the challenges and opportunities faced by small businesses in the context of internal controls. These discussions allow the development of recommendations for small business controls. From these recommendations a research agenda for an extensive future examination of these issues is proposed. This proposed, future research agenda is described in the following section.

5.0 A proposed research agenda

From the above discussion there appears to be a need for a systematic research agenda regarding the development and use of accounting internal controls and control systems in small businesses. What follows below is a proposed agenda for research exploring these small business issues. The initial step is to provide a structure for the research. An appropriate structure is the COSO (Committee of Sponsoring Organizations) framework ("Committee of Sponsoring Organizations of the Treadway Commission", 2013). What follows is a brief overview of the COSO framework.

The COSO framework defines five components, control environment; risk assessment; control activities; information and communication; and monitoring activities. These five components would each be evaluated to assess the effectiveness of small businesses regarding security and controls to address potential fraud. The control environment consists of standards, processes, and structures providing the basis for organizational activities. Examples include organizational governance and structure, the defined patterns of authority and responsibility, methods of performance evaluation and incentive structures, and the industry environment. Risk assessments are the processes throughout the business used to identify the factors that might keep the business from achieving its objectives. Control activities are policies, processes, and procedures designed to help assure risks are mitigated in organizational activities. Examples of the broad categories of control activities include authorization, reconciliation, adequate documentation, physical security, and segregation of duties. The fourth component is information and communication which focuses on the processes and procedures used to collect and disseminate internal as well as external information throughout the business needed to support the achievement of its objectives. The final component in this framework is monitoring activities which are the on-going assessments and evaluations regarding the effectiveness of the internal controls which the business employs.

5.1 The target population

Given the above five component framework, the next step in the research agenda is to identify an appropriate collection of small businesses and the corresponding owners or senior managers. A variety of small business definitions exist and a decision must be made as to which definition to employ. Often the business dimension used to define the size of the organization is the number of employees. The selection of this definition needs to be done carefully. A too stringent definition (e.g., small employee number requirement) and the target population and data sample would be very small. Yet if defined too broadly (e.g., too large number of minimum employees) the target population and data sample could lack meaningful homogeneity. One reasonable employee size to use as a cutoff to define a small business is 100 employees or less. This would hopefully provide a sufficiently large yet homogeneous target population.

5.2 Identifying the issues faced by small businesses

In order to understand the security, compliance, and internal control issues faced by small businesses, it would best to interview a collection of small business owners or senior managers selected from the target population. Given scheduling requirements and the demands on these owners and managers, individual interviews maybe needed rather than using focus groups. However, if such scheduling is feasible, a series of focus groups would be efficient.

Regardless of the method used, individual interviews or focus groups, a series of open-ended questions would be asked of these owners or managers. These questions would be organized around the COSO framework in each of the five component areas. For example in the control environment component these questions would focus on understanding the organizational structure and corresponding authority and responsibilities for jobs in the business. Additional questions could examine how organizational governance takes place and the influence of the industry environment on governance and organizational structures. Another example of these questions could be how employees are recruited, evaluated, and rewarded.

The second COSO framework component is risk assessment. Example questions to ask the owners and managers would focus on identifying the critical success factors (i.e., activities key to achieving business objectives) and the variables influencing these factors. Critical success factors would be in a variety of organizational areas such as financial, operational, reporting, and compliance. These questions and answers would elicit from the owners and managers the processes used in their businesses to identify and monitor these critical success factors and appropriately adjust activities in response to any identified risks.

Control activities are the third component of the COSO framework. The questions posed to small business managers and owners would be structure along two dimensions, accounting cycles (e.g., revenue, expenditure, payroll, fixed asset, financing and administrative) and internal control type (e.g., authorization, reconciliation, adequate documentation, physical security, and segregation of duties). The questions would ask owners and managers specific examples of potential fraud and corresponding internal controls. The questions to elicit information within the final two COSO framework components would focus on information and communication as well as monitoring activities. The information and communication questions would examine what data are collected as well as the dissemination method and frequency of the resulting information based on this data. The goal would be to support the achievement of business objectives and control. The questions focusing on the monitoring component would examine how the business uses the disseminated information to systematically identify meaningful variances between actual and desired performance and to take corrective action as needed.

Throughout these interviews or focus groups, ideally the owner and managers' responses would be recorded and ultimately transcribed to text. Once in text form, content analysis could be applied to these responses and comments. Content analysis would allow the systematic identification of themes and subthemes and hopefully grounded theory developed across all the owners and managers responding to the questions.

5.3 Data collection and analysis

Building on the results from the content analysis, a series of questionnaire items would be developed providing meaningful coverage of the domains of the identified themes, subthemes, and grounded theory constructs.

Questionnaire items could be selected and modified from the literature. Other items would be written, as needed, by the researcher. The questionnaire items would be organized into a formal questionnaire and the questionnaire pretested on an appropriate group of small business owners and managers. Based on the feedback from this pretest, the questionnaire can be finalized for distribution to the target population.

The questionnaire could be distributed either via traditional mail or the Internet or both. The key to developing an appropriate sample is the list of potential respondents invited to complete the questionnaire. This list could be purchased or obtained or developed from free sources (e.g., Small Business Administration). Once the sample of responses are compiled, a variety of analyses can be performed. These could range from descriptive and exploratory analyses to structural equation modeling, given appropriate theory or grounded theory from the content analysis is identified.

5.4 Potential manuscript topics

The manuscripts which could be developed from this proposed research program are in a number of areas. Several of the potential manuscripts would focus on the issues and problems faced by small businesses. These manuscripts would make contributions in the small business management literature. Another set of manuscripts would examine accounting cycles and internal controls in small businesses. These manuscripts have the potential to make contributions in the accounting controls and accounting information systems literatures.

6.0 Summary

The focus of this manuscript is to illustrate the fraud, security, and control issues faced by small businesses. Losses of financial resources due to fraud are significant and growing in magnitude. Such losses are particularly harmful for small businesses as a percentage of their total resources. Making matters worse, characteristics of small businesses make them ripe targets for fraud and create barriers to fully implementing appropriate security and controls to address fraud. Examples of these barriers include limitations in resources and expertise and often too few employees to fully implement traditional internal accounting controls (e.g., segregation of duties).

The method used in this manuscript was to develop conceptual arguments regarding the issues based on the literature. These arguments allow a discussion of recommendations for small business control. The manuscript concludes with a proposed, future research agenda to examine the issues of small business fraud, security, and control in a systematic fashion. Through such research, practical recommendations may be provided to small business owners and managers to combat fraud and security threats.Small businesses face unique issues and constraints regarding fraud, security, and compliance when compared to larger organizations. Studying small businesses within the context of fraud, security, and controls provides a better understanding of small business operations and compliance.

References

8 Simple Internal Controls for Small Businesses. (2008). Retrieved from http://www.chiefexecutiveblog/2008/10/8-simple-internal-controls-for-small.html accesses 02/23/2016.

2016 ACFE Report to the Nation. (2016). Retrieved from http://www.acfe.com/rttn2016/about/ececutive-summary.aspx accessed 5/18/2016.

Committee of Sponsoring Organizations of the Treadway Commission. (March 2013). Internal Control-Integrated Framework, Executive Summary.

Dawson, S., (2015). Internal Control/Anti-Fraud Program Design for Small Business: A Guide for Companies Not Subject to Sarbanes-Oxley Act. Hoboken NJ: John Wiley & Sons. http://dx.doi.org/10.1002/9781119083733

Effective Internal Control for Small Medium Business. (n.d.). Retrieved from http://accounting-financial-tac.com/2009/04/effective-internal-control-for-small-medium-business accessed 2/23/2016.

Hess, M., Contrell, Jr., J., (2016). Fraud risk management: A small business perspective. Business Horizon, 59(1): 13-18. http://dx.doi.org/10.1016/j.bushor.2015.09.005

Hibbert, R., (2012). SMBs and the struggle for compliance. Computer Fraud & Security, 11: 5-7. http://dx.doi.org/10.1016/S1361-3723(12)70112-4

Internal Controls-Keys to Business Success. (n.d.). Retrieved from http://www.sba.gov accessed 2/23/2016.

Jackson, K., Holland, D., Albrecht, C., Woolstenhulme, D., (2010). Fraud isn't just for big business: Understand the drivers, consequences and prevention of fraud in small business. The Journal of International Management Studies, 5(1): 160-164.

Laufer, D., (2011). Small business entrepreneurs: A focus on fraud risk and prevention. American Journal of Economics and Business Administration, 3(2): 401-404. http://dx.doi.org/10.3844/ajebasp.2011.401.404

Spencer, R., (n.d.). Internal Controls for Small Business Accounting. Retrieved from http://www.wbrauncpa.com/Documents/Internal%20Controls%20for%20Small%20Business%20Accounting.pdf accessed 06/02/2016.

Turner, L. andWeickgenannt, A. (2013). Accounting Information Systems: The Processes and Controls, 2nd Edition. Hoboken, NJ: John Wiley & Sons.