A Process Improvement Framework for Information Technology Management in Small to Medium Enterprises (PI4IT)

Thomas J. Bilan
tom.bilan@bilan.com

S. Alan McCord
amccord@ltu.edu

College of Management
Lawrence Technological University
Southfield, MI 48075, USA

Abstract

Small to Medium Enterprises (SMEs) account for over 99.7% of businesses in the U.S. and over 95% globally. 90% of those SMEs use computer systems as part of daily business operations. Despite the high penetration of Information Technology (IT) at the SME level, many SMEs lack proper IT management practices. For example, studies have shown that seven out of ten SMEs go out of business after a major data loss event. Proper IT management guidance can mitigate or eliminate many SME IT management issues.

This paper focuses on the development and validation of the Process Improvement for Information Technology (PI4IT) framework and its accompanying assessment model. PI4IT addresses and improves many common SME IT issues through the assessment and accomplishment of goals across seven foundational capabilities. The foundational capabilities were determined using a Delphi methodology and validated using mixed methods techniques using survey data collected from 72 SME IT providers and practitioners.

Keywords: IT Management, IT Process Improvement, SME, Foundational Capabilities

1. INTRODUCTION

Poor Information Technology (IT) management practices claimed another victim. The Kontiki Tanning Salon, a thriving single location small business, was forced to cease its operations. Its fate was not due to a natural disaster, poor customer service, or increased competition. An inexpensive commodity desktop hard drive contained the only copy of its accounting and customer information, especially the critical details about its clients' prepaid tanning packages, suffered a catastrophic failure. Kontiki, no longer having knowledge of which clients owed them money or when their tanning packages expired, went out of business because they could no longer support their customers. Their computer system was so efficient that they never considered printing reports, thus they had no business contingency plan in the event of a critical IT failure. The most disappointing fact was that Kontiki had a tape backup installed in the system but neglected to use it. Like seven out of ten other SMEs that suffer a major data

loss event, Kontiki ended up closing their doors (Hewlett Packard, 2007).

The Kontiki case underscores that SMEs are often unaware of how vulnerable their businesses are to improperly managed IT. Chao and Chandra (2012) discuss owner's IT knowledge for small US business and the positive correlation between their IT knowledge level, IT strategic alignment and IT adoption. It stands to reason that the lack of IT knowledge would be associated with an increased naivety towards IT management, the results of which can lead to disastrous business consequences. Surely the Kontiki case study would support this theory.

Owners are still deeply involved with their businesses as they begin to transition to SME status. Often owners are still directly involved with IT decisions even after they begin relying on others in the organization to perform IT related functions. Regardless of the owner's IT knowledge, the PI4IT survey results in Figure 1 state that 57 of 63 SMEs owners are involved in IT spending decisions. These owners are using their understanding of IT to make decisions, some of which can be risky, expensive and devastating when wrong, on how to best invest in technology that will align with their business strategy. Providing SME owners with IT knowledge and a plan for IT improvement can help them make better IT management investment decisions.

The Process Improvement for Information Technology (PI4IT) framework was created to help SMEs identify IT management weaknesses and offer suggestions to improve their capabilities. This paper summarizes the PI4IT framework, which is tailored to address the most common SME IT management concerns. These management concerns are grouped into 7 different categories: Backup, Disaster Recovery, Hardware, IT Strategy, Networking and Internet Technologies, Security, and Software.

PI4IT was created through research conducted using a Delphi panel of SME IT Management experts and was validated through a survey comprising 72 SME participants. PI4IT is free to use and a simple checklist is available at www.pi4it.com and in Appendix B.

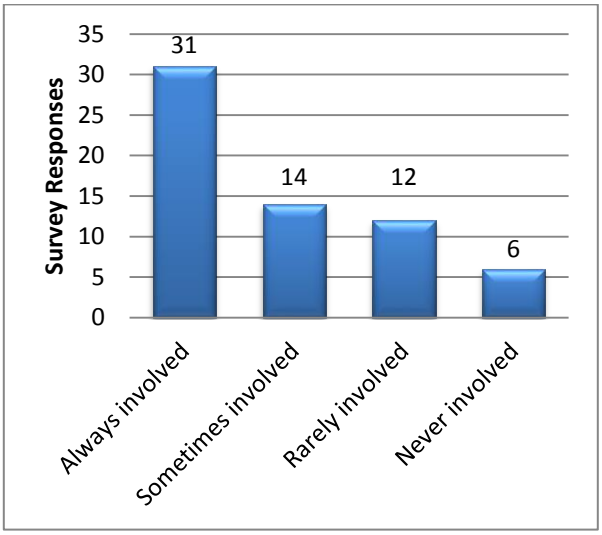


Figure 1. Owner involvement in IT spending decisions.

This paper is organized into several sections. The Literature Review section provides an overview of SME IT and other IT management industry frameworks. The PI4IT Overview and Terminology section prepares the reader for the different PI4IT concepts presented in subsequent sections. The Proposition section provides the hypothesis used to validate the PI4IT framework. The Research Design and Procedures section details the validation method and statistical tests. The Research Findings section provides additional insight from survey results. The Conclusion and Future Research sections reinforce the validation of the PI4IT framework and detail several ideas for future research.

2. LITERATURE REVIEW

IT management is often an overlooked function of SME business strategy. In the U.S., there are about 26 million SMEs (Small Business Association, 2009) and about 91 percent of them use computers for business operations (Tarabishy, 2007). Many SMEs equate computer repair with IT management and this reactive versus proactive approach can lead to disaster. Many SME business owners believe that if their computer breaks they can just replace it the same they replace their copier, vehicle, or cell phone. Most of the value of the computer system is in the information that it stores and the business logic it automates, not the replacement cost of the hardware.

Silvius (2004) explains that the typical SME uses IT for traditional administration functions but often does not integrate IT into the strategic elements of the company and thus the lack of strategic integration causes SMEs to lag behind large enterprise in productivity improvements. Several other studies focus on the importance of IT adoption in the SME as a facilitator of continued growth and development, which increases the SME's chances for survival (Lester & Tran, 2008; Dans, 2001). Silvius (2004) describes IT management as "…done on a 'crises by crises' basis which causes SMEs to be in a constant crisis reactive mode versus a structured and predictable proactive mode." SME IT Management does not want to, or at least should not need to, be synonymous with crisis management.

SME IT management has grown from a very small and niche issue in the 1980s to a billion dollar problem today. As technology continue to integrate our society via social networking, banking, communications, business automation, and other functions, an increasing number of SMEs will adopt IT at various strategic levels in their organizations. As SMEs adopt IT systems they become an important part of business processes and their ability to perform their function effectively becomes business critical.

Despite the size and scope of the SME IT management market, there was the lack of a process improvement framework targeted at common SME IT management issues. With as many as seven out of ten SMEs going out of business within a year of a major data loss event (Hewlett Packard, 2007), it is apparent that the existing IT management efforts are not adequate. Research and development of a framework that addresses the specific IT management needs of the SME has the potential to positively affect millions of SMEs globally.

Industry Frameworks

A discussion of other major industry frameworks and some of their derivatives are provided in this section. PI4IT's meta structure was inspired by the staged maturity approach of CMM/CMMI (Software Engineering Institute, 2009; Software Engineering Institute, 2007; Software Engineering Institute, 2006) and the benchmarking capabilities and activity goals of COBIT (IT Governance Institute, 2007). PI4IT makes its contribution in tandem with these other frameworks by researching and developing a new framework designed from the inception for SMEs.

CMMI

Capability Maturity Model Integration (CMMI) models include in them a number of best practices that "help organizations improve their processes" (Software Engineering Institute, 2007). Originally developed to help companies improve processes over the entire life cycle of product development and service provision from conceptualization to disposal, other CMMI protocols were also developed to address issues such as the "acquisition environment" (CMMI-ACQ) and for development (CMMI-DEV) (Carnegie Mellon, p. 3).

The Software Engineering Institute (SEI) created the first CMM designed for software organizations in Capability Maturity Model: Guidelines for Improving the Software Process (1995). Because of the evolution of CMMI, a model foundation (CMF) for all CMMI gradually emerged, entailing components required to be in every model generated in the framework.

A CMM framework is composed of numerous process areas, defined as "a cluster of related practices in an area that, when implemented collectively, satisfies a set of goals considered important for making improvement in that area" (Software Engineering Institute, 2009). Various process areas within the model all have required, expected, and informative elements. These processes can be illustrated by various pathways with a staged representation of them emphasizing maturity levels in the processes, "whereas the continuous representation utilizes capability levels" (Software Engineering Institute, 2009).

A capability level (marked as ranging from incomplete to managed, defined, quantitatively managed or optimizing) and maturity level dimensions (marked as ranging from initial to optimizing) of CMMI are used for the purpose of benchmarking and appraisal activities, "as well as guiding an organization's improvement efforts" (Software Engineering Institute, 2007). With regard to capability levels, it is only at level 4 that the process area becomes "a key business driver that the organization wants to manage using quantitative and statistical techniques" (Software Engineering Institute, 2007). PI4IT has achievement levels that are similar to CMMI capability levels.

A maturity level is rather a group of practices "for a predefined set of process areas that improve the organization's overall performance" and as such provides a way to predict organizational performance (Software Engineering Institute, 2007). Reviewing these levels, one gains insight to some maturity problems in companies as level one is "ad hoc and chaotic" in which one has "a tendency to over commit" or abandon processes, with management of processes only emerging in level 2. At level 3, when maturity becomes defined, "the procedures for a project are tailored from the organization's set of standard processes to suit a particular project or organizational unit" (Software Engineering Institute., 2007). As one climbs the maturity levels, predictability of process performance through the use of statistical and quantitative techniques finally leads to an optimizing maturity level at which one is able to "continually (improve) process performance through incremental and innovative process and technology" primarily because the optimizing allows the organization to address causes of process variation and thus improve process performance (Software Engineering Institute., 2007).

In addition to mapping out a path of process improvement, appraisal is also a critical part of the process with the SCAMPI method being the most commonly used method to appraise organizations using CMMI (Software Engineering Institute, 2007). This method results in maturity level ratings, capability level profiles, and an achievement profile, which helps organizations track their progress through the stages. Similar to CMMI, PI4IT's also includes a quick assessment method to identify an organizations achievement level for each foundational capability.

The CMMI framework's influence on this research is CMM/CMMI's success for improving process by using a staged maturity rating approach. In addition, there are structural parallels between the hierarchy of the CMMI process area, and its related goals, and the PI4IT foundational capability, and its related goals. PI4IT's development specifically addressed the SME's needs by being reasonable, convenient, practical, and feasible versus the CMM/CMMI frameworks that often required dedicated staff and a significant amount of time and funding.

COBIT

Increasingly, businesses are recognizing the importance of IT to their success, meaning that more and more managers are now seeking to manage IT risks and control their IT operations: a process now termed IT governance (IT Governance Institute, 2007). IT Governance Institute (2007) argued that for the most part "it is responsibility of the executives and the board of directors" to provide a company with IT governance, and that they must lead the company in developing the "organizational structures and processes that ensure that the enterprise's IT sustains and extends the organization's strategies and objectives" (IT Governance Institute, p. 5).

The Control Objectives for Information and Related Technology (COBIT) framework is useful as a process framework and structure to optimize IT-enabled investments (IT Governance Institute, 2007). COBIT organizes all of a company's IT activities "into a generally accepted process model" as well as identifies IT resources to be leveraged and management control objectives to be considered (IT Governance Institute, 2007).

COBIT functions by dividing IT into four domains and 34 processes to provide an end-to-end view of IT in any given company. COBIT determines and monitors IT performance levels by using benchmarking based on the SEI's CMM, measuring outcomes based on Kaplan and Norton's balanced business scorecard and deriving control objectives or activity goals in order to get all processes under control (IT Governance Institute, 2007). Moreover, "the assessment of process capability based on the COBIT maturity models is a key part of IT governance implementation" (IT Governance Institute, p. 6).

Without detailing specific COBIT products available for personnel at all levels of corporations, IT Governance Institute (2007) remarked that overall COBIT "enables the development of clear policies and good practice for IT control throughout enterprises" (2007). Not only does it provide a better understanding among most stakeholders of what IT can do for the company, but also COBIT is generally accepted among many third parties, regulators and other stakeholders, and thus has become a common language in the field of IT governance.

IT Governance Institute (2007) described in detail how the COBIT framework entails

acquiring, implementing, delivering, supporting, monitoring, and evaluating IT use in terms of capabilities and maturity levels within an organization. In addition to process controls, COBIT also entails systems development, change management, security, and computer operations.

COBIT appraises progress in various processes by utilizing the maturity model developed by the SEI in the context of CMM, but making the maturity modeling benchmarks more general so that they go beyond the SEI measures according to software product engineering principles to apply to numerous management processes. COBIT also only uses maturity models to describe "possible current and future states" and does not use them according to the CMM threshold model whereby one cannot move to the next higher level without fulfillment of lower level requirements, and also, "with COBIT's maturity models, unlike the original SEI CMM approach, there is no intention to measure levels precisely or try to certify that a level has exactly been met" as COBIT only seeks to create a profile "where conditions relevant to several maturity levels will be met" (IT Governance Institute, 2007). This allows managers to compare where their company stands as opposed to other companies in the field, and to formulate a growth path from as-is to to-be. Overall, the COBIT framework, "ties the business requirements for information and governance to the objectives of the IT services function" (IT Governance Institute, 2007).

COBIT Quickstart

The size and scope of the COBIT IT governance framework's 34 processes, 210 control objectives, 17 generic business goals, and 28 generic IT goals can be overwhelming for smaller companies. COBIT Quickstart was developed based on the "need of IT managers of smaller organizations for a simple-to-use tool that will speed up the implementation of key IT control objectives" (IT Governance Institute, 2007). COBIT Quickstart provides a limited number of processes, 32 vs. 34, and control objectives, 59 vs. 210, that are deemed more applicable to smaller environments.

COBIT is a mechanism used by many companies to achieve Sarbanes-Oxley (SOX) compliance. SOX compliance can cost small public companies as much as "ten times more than what it does for large enterprises" (Armstrong, 2008). The Sarbanes-Oxley Compliance Journal states that COBIT Quickstart provides a mechanism for small public companies with "IT shops with fewer than 10 employees should look at COBIT Quickstart" (Armstrong, 2008).

COBIT Quickstart is the closest framework in size and scope to PI4IT but it is still too cumbersome for many small enterprises. A comparison of COBIT Quickstart framework's control objectives and PI4IT's goals determined that COBIT Quickstart had roughly 20 control objectives that were deemed out of PI4IT's scope or not providing enough value to PI4IT's target audience. In addition, the COBIT Quickstart assessment checklist is thirty-one pages whereas PI4IT has seven pages. PI4IT's smaller size makes the framework more applicable and approachable by companies just beginning to investigate or employ IT management process improvement. COBIT Quickstart would be a possible subsequent framework for SMEs that attain achievement level four on all foundational capabilities.

3. PI4IT OVERVIEW AND TERMINOLOGY

The core tenets of the framework are introduced in the following subsections.

Foundational Capability

A foundational capability within PI4IT is a set of related functions, processes, abilities, or capacities that addresses an IT management domain. The common IT management concerns were grouped and then assigned to a foundational capability. Each foundation capability addressed several common IT management concerns and was the target for process improvement. A foundation capability is analogous to a CMMI process area or a COBIT domain. A foundational capability may also be referred to as an IT management category.

Meta Model

The UML meta model in Appendix A describes the meta structure behind the PI4IT framework. The top level of the framework contains a set of foundational capabilities. Each foundational capability addressed an overall IT management theme, such as Security. A foundational capability has four achievement levels, each representing a plateau of maturity. These achievement levels contained goals designed using certain principles and refined through practitioner and provider feedback.

In practice, the SME was able to choose which foundational capabilities they wanted to address. The SME used the assessment process, provided in Appendix B, to determine their current achievement level for each foundational capability. The assessment process identified capability gaps, which were then prioritized and reconciled through the accomplishment of goals.

Achievement Levels
Achievement levels are a method of subdividing the foundational capabilities into manageable sets of goals. Each achievement level contains one or more goals that build upon earlier goals and have similar levels of complexity. Figure 2 shows a graphical representation of the achievement levels.

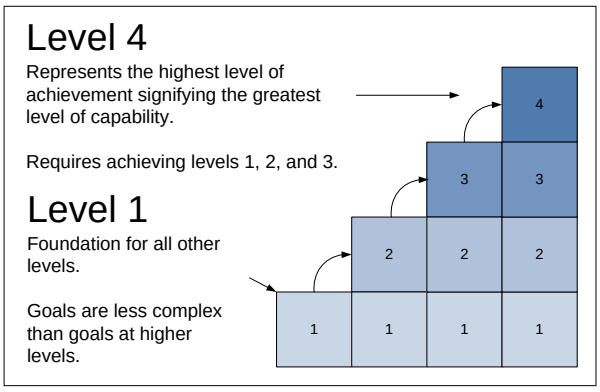


Figure 2. Achievement Level Progression

4. PROPOSITION

The research proposition was that the performance of IT for delivery of foundational capabilities in SMEs could be improved using a framework, tailored to guide the SME through the IT management improvement process. This proposition was validated by the survey question that asked if accomplishing the goals at the next higher achievement level would have the potential to improve capability.

5. RESEARCH DESIGN AND PROCEDURES

The research was conducted in four phases:
1. Determine IT Management Categories
2. Build Framework
3. Collect Survey Data
4. Analyze Survey Data

Phase 1: Determine Foundational Capabilities
The seven foundational capabilities are the primary sections of the PI4IT framework. These IT management categories were determined by using the Delphi method with a group of 8 SME IT Management experts, each with over 10,000 hours of career IT management experience. The Delphi method was chosen because of its ability to reach a consensus through multiple iterations and its ability to avoid bias through inter-expert anonymity.

The SME IT experts participated in two rounds of Delphi surveys. The first round featured an open-ended question asking each expert what the top 5 SME IT management issues. The results were qualitatively interpreted into what resulted in 10 different categories. A second round of surveys asking to rank the results from round one resulted in 7 final categories being chosen for PI4IT.

Phase 2: Build Framework
The Delphi process resulted in the following seven IT management categories: Backup, Disaster Recovery, Hardware, IT Strategy, Networking and Internet Technologies, Security, and Software. Each IT management category is composed of several goals. Goals are sorted into four achievement levels based on complexity. Level 1 goals are relatively easy to accomplish while level 4 goals are significantly more difficult.

Phase 3: Collect Survey Data
Survey data was collected from the eight member Delphi expert group and a convenience sample of 72 SME IT managers. Each member of the Delphi expert group was notified via e-mail requesting their participation in the framework validation survey and this resulted in 100% survey participation. Additionally, a convenience sample of SME business owners and IT Managers was collected by encouraging IT Managers to evaluate the PI4IT Quick Assessment checklist and then take an online survey. The convenience sample consisted of members of SME IT management groups on LinkedIn, hundreds of members of the Monroe County Chamber of Commerce, anonymous web-based users that found the PI4IT web site, IT Manager colleagues of the Delphi expert group, and IT Manager colleagues of the researcher.

Phase 4: Analyze Survey Data
The research proposed that the performance of IT for delivery of foundational capabilities in SMEs could be improved through a framework tailored to guide the SME through the IT

management improvement process. The key phrase for proposition validation is "could be improved." Thus, a specific survey question used to validate the hypothesis asked if accomplishing the goals at the next level up would improve management capability.

The survey question used a common five point symmetric Likert scale where the median value represented a neutral value. The results were scored according to the values in Table 1. The hypothesis (H_1) was that the framework had the potential of capability improvement. This was equivalent to a mean score of 3.5 or higher.

Likert Survey Option	Numeric Score
A definite capability improvement	5
Some capability improvement	4
No improvement	3
Some capability reduction	2
A definite capability reduction	1

Table 1. Likert Wording and Associated Value

The Wilcoxon signed-ranks test was selected for statistical validation. The Wilcoxon signed-ranks test is a single sample non-parametric test used to determine before and after effects. The equivalent parametric test is the common single-sample t-test. Sheskin (2004) states that the Wilcoxon Signed-Ranks test has an asymptotic relative efficiency of .955 when compared to the single-sample t-test. Thus at a power of .8, a single-sample t-test of 95 subjects has about the same power as the Wilcoxon signed-ranks test with 100 subjects.

The value of "No improvement" signified that the framework neither increased nor decreased capability. The hypothesis of $H_1 > 3$ represented that the framework was effective and had the potential to improve capability at the next level up.

The customary acceptance criterion of $\alpha = .05$ was deemed adequate to determine if significant evidence exists to reject H_0.

Stata/SE version 10.0 was used to compute the Wilcoxon signed-rank for the 235 survey responses across all seven foundational capabilities. The summary of the test results are provided in Table 2.

Foundational Capability	*z* score	One-tail Probabil	Reject H_0
	@ H_0 = 3	ity	
Backup	5.604	.0000	Yes
Security	5.505	.0000	Yes
Hardware	4.392	.0000	Yes
Software	4.802	.0000	Yes
Disaster Recovery	5.522	.0000	Yes
IT Strategy	5.379	.0000	Yes
Networking and Internet Technologies	4.918	.0000	Yes

Table 2. Summary of Wilcoxon Statistical Test Results

An analysis of the Wilcoxon signed-rank results in Table 2 showed that the framework has the potential to improve IT for delivery of foundational capabilities in SMEs significantly greater than $\alpha = .05$ level of significance. In fact, the results were so positive that the minimum significance level across all seven foundational capabilities was z = 4.392. That is equivalent to having one out of every 178,073 companies who implement the framework actually reduce their capabilities.

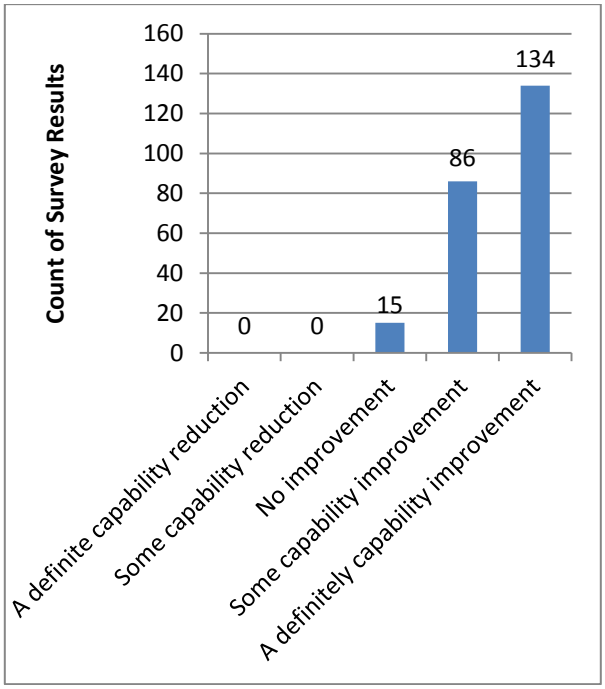


Figure 3. Extent to which accomplishing the goals at the next level would improve capability

Figure 3 is a histogram of every response relating to the framework's ability for capability improvement across all seven foundational

capabilities. Of the 235 survey responses, the number of people who chose the option that a foundational capability would actually result in decreased capability was zero. Every other response was neutral or positive. A visual inspection of Figure 3 shows overwhelming support from 220 of the 235 responses which shows that the framework does have the potential to improve capability.

6. RESEARCH FINDINGS

This research provided insights via two independent survey groups. The first survey group was the Delphi expert group, which was surveyed to determine if the framework was ready for general release. The Delphi expert group favored the framework with good scores overall and some useful feedback that was used to refine the framework. The second survey group consisted of practitioners and providers. Their opinions reaffirmed those of the Delphi expert group by confirming the expected effectiveness of the PI4IT framework.

Although PI4IT accomplished its goal of improving IT performance for the development of foundational capabilities, PI4IT appears to support business strategy and may enable SME IT managers to identify improvement projects based on PI4IT's goal statements. This section provides an analysis of the survey data with respect to these areas.

PI4IT's Capability to Support Business Strategy

Each foundational capability was rated as to its potential to improve the capability to support business strategy. Figure 4 shows how each foundational capability scored. Although every foundational capability provided strong results, the best performers include Software and IT Strategy with over 90% of the respondents expressing that those categories have high potential to improve the capability to support business strategy. Figure 5 shows the percentage broken down as some potential and higher versus some low potential and lower.

PI4IT's Capability of Improving IT Management Performance

The analysis performed in Phase 4 provided overwhelming statistical support for accepting the hypothesis using the Wilcoxon signed-ranks test for ordinal data. Additionally, hypothetically changing the assumption that the Likert data was of interval format and performing validation tests using the parametric single sample t-test results in the same conclusion. Thus, every foundational capability in the framework provided the potential to improve performance of IT for the delivery of foundational capabilities in SME.

SME Ability to Identify Improvement Projects

Even though almost all IT Managers agreed that accomplishing the goals at the next level up would improve capability, many of them had issues identifying projects to accomplishing these goals. A survey question asked "…to what extent can you identify specific projects that will help you achieve the remaining goals?" This question was a measure of SME IT Managers' background, skills, and experience relative to each foundational capability.

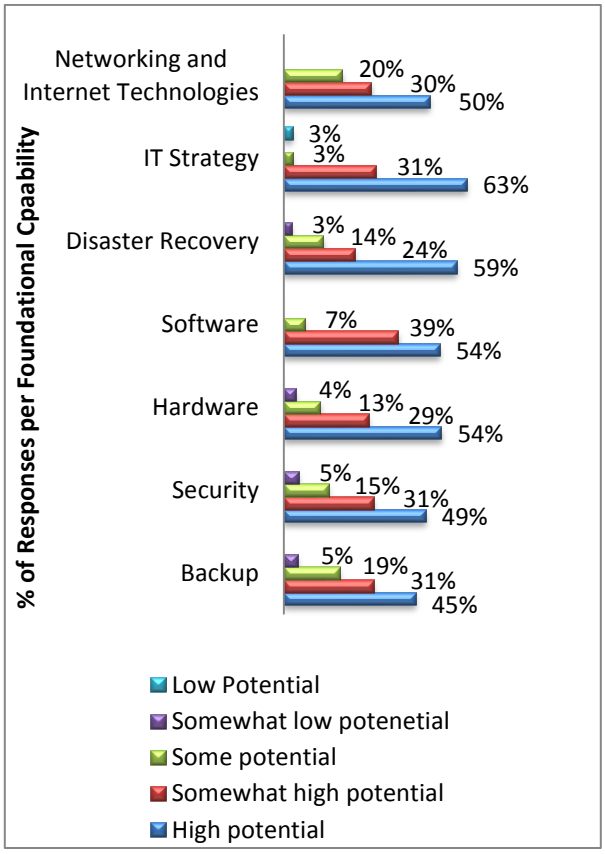


Figure 4. Potential for PI4IT to Support Business Strategy

ISSN: 2167-1508
v6 n2815

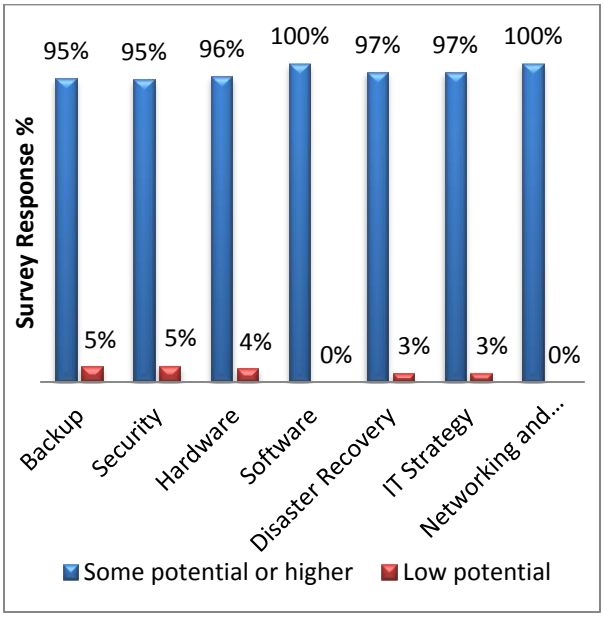


Figure 5. Survey results about potential for framework to support business strategy.

Figure 6 and Figure 7 are charts of the survey responses pertaining to the ability to identify projects. Several observations were made:

- Virtually no respondents said, "I'm not sure where to start" (3 of 235 responses), showing that the respondents understood the foundational capability and could minimally envision somewhere to start for improvement.
- Backup and Security appeared to be areas where people had a difficult time identifying projects.
- The majority of respondents identified at least one or more specific places to start for all foundational capabilities.
- Hardware and Software projects appear to be the easiest for SME IT managers to identify.

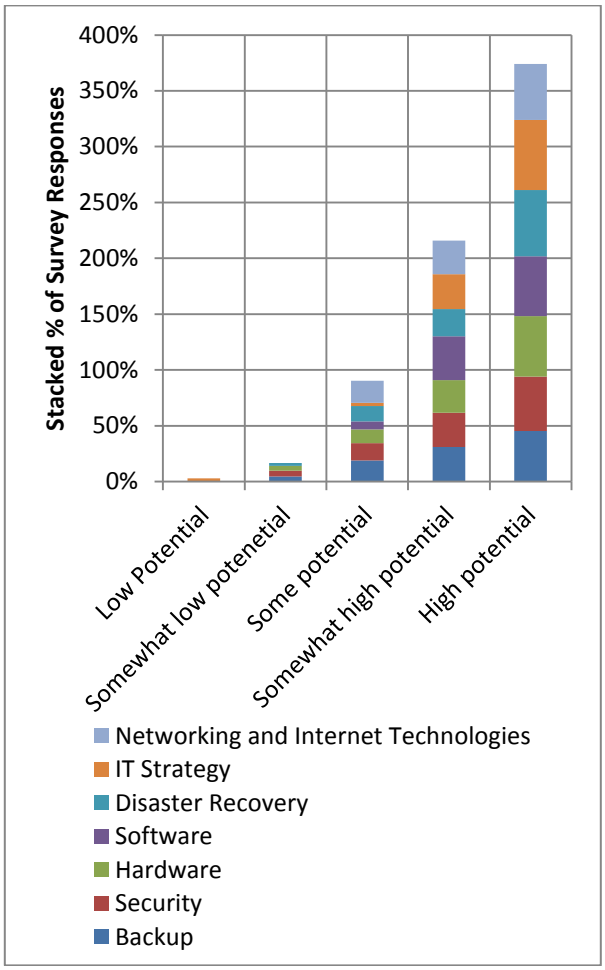


Figure 6. Survey results about PI4IT's potential to support business strategy

7. CONCLUSIONS

Statistical tests were performed on the foundational capabilities individually and then performed on the framework holistically. The hypothesis claimed that the framework does statistically have the potential for SMEs to improve the performance of IT for delivery of foundational capability. The statistical analysis provided significant evidence to support the proposition at an $\alpha > .01$ level of significance. The quantitative analysis overwhelming supports that the PI4IT framework is an effective and useful tool for improving IT performance for SMEs.

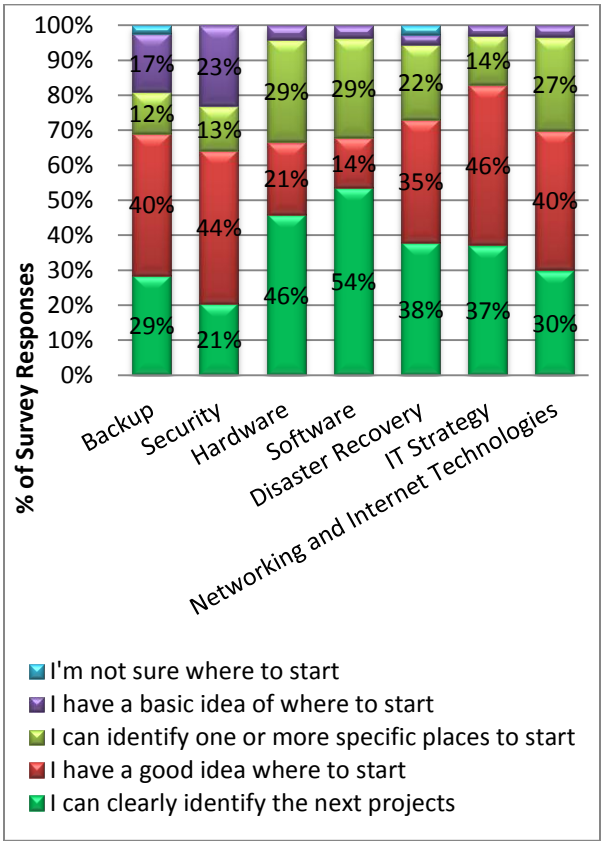


Figure 7. Survey results about respondent's ability to identify projects per foundational capability

8. FUTURE RESEARCH

The PI4IT framework provides many different opportunities for future research. The most obvious opportunity is to expand the number of foundational capabilities and goals. Other possibilities include the creation of a hierarchy of foundational capabilities or integration of risk, cost, prioritization, and capacity as factors.

Validation After Implementation
This paper analyzes PI4IT's as a function of the perception of its potential efficacy. A longitudinal study could be performed to validate PI4IT's effectiveness once actually implemented.

Increasing the Number of Foundational Capabilities, Goals, or Levels
PI4IT's meta-structure is extensible. Additional foundational capabilities and goals are capable of being added or removed without redesigning the core structure. It is even possible to add additional achievement levels, although this is discouraged because all foundational capabilities currently have four levels for convenience and consistency. As an example, Telecommunications or Archiving could be added as foundational capabilities.

Another possibility for new categories that may be related to an existing foundational capability, such as how Archiving could be considered related to Backup, is to define the concept of adjunct capabilities extensions. For example, goals for Archiving can be added to the existing Backup foundational capability to create a Backup+ foundational capability instead of a separate Archive foundational capability.

Linking Foundational Capabilities and/or Goals
Foundational capabilities are independent but loose relationships can exist between goals in multiple foundational capabilities. For example, a level two goal for the Software states, "Compare hardware specifications with software requirements." The level one goal for Hardware is, "Build a thorough hardware inventory including hardware specifications." Although these goals are capable of being completed independently, the Software goal is accomplished easier if the Hardware goal is first completed.

Foundational capabilities can be hierarchical. Logical progressions such as a requiring an achievement level four rating in the Backup foundational capability could be a third or fourth level goal for the Disaster Recovery foundational capability.

Integration of Risk, Cost, Prioritization and Capacity
Currently, the PI4IT framework does not account for factors such as risk, cost, prioritization, and capacity. These factors are considered implicit in the evaluation of the goals to be addressed by the practitioner. Integration of these factors into PI4IT is certainly possible. One method would be to research existing literature around a goal or set of goals and then populate values into PI4IT for risk, cost, prioritization, and capacity. Another way of collecting data for these factors would be through opinions of other providers and practitioners through surveys or forums available on the PI4IT web site. In addition, if the PI4IT web site were extended to provide a tracking tool where many practitioners and providers tracked their own values then

some community statistics could be computed and used as baseline values for these factors.

9. REFERENCES

Chao, C-A, & Chandra, A. (2012). Impact of owner's knowledge of information technology (IT) on strategic alignment and IT adoption in US small firms. Journal of Small Business and Enterprise Development. Vol 19. No 1, 114-131.

Dans, E. (2001). IT Investment in Small and Medium Enterprises: Paradoxically Productive? The Electronic Journal of Information Systems Evaluation , 1-15.

Hewlitt Packard. (2007). Impact on U.S. Small Business of Natural & Man-Made Disasters. Retrieved July 27, 2010, from SCORE: http://www.score.org/pdf/HP_Download_ImpactofDisaster.pdf

IT Governance Institite. (2007). Cobit 4.1. Rolling Meadows, IL: IT Governance Institute.

IT Governance Institute. (2007). CobiT Quickstart: 2nd Edition. Rollilng Meadows, IL: IT Governance Institute.

Lester, D. L., & Tran, T. T. (2008). Information Technology Capabilities: Suggestions for SME Growth. Journal of Behavioral and Applied Management , 72-88.

Software Engineering Institute. (2007). CMMI for acquisition, Version 1.2. Carnegie Mellon University.

Software Engineering Institute. (2006). CMMI for development, Version 1.2: improving processes for better products. Carnegie Mellon.

Software Engineering Institute. (2009). CMMI for Services, Version 1.2. Pittsburg, PA: SEI.

Small Business Association. (2009). Frequently Asked Questions. Retrieved June 3rd, 2009, from Small Business Administration: http://web.sba.gov/faqs/faqIndexAll.cfm?areaid=24

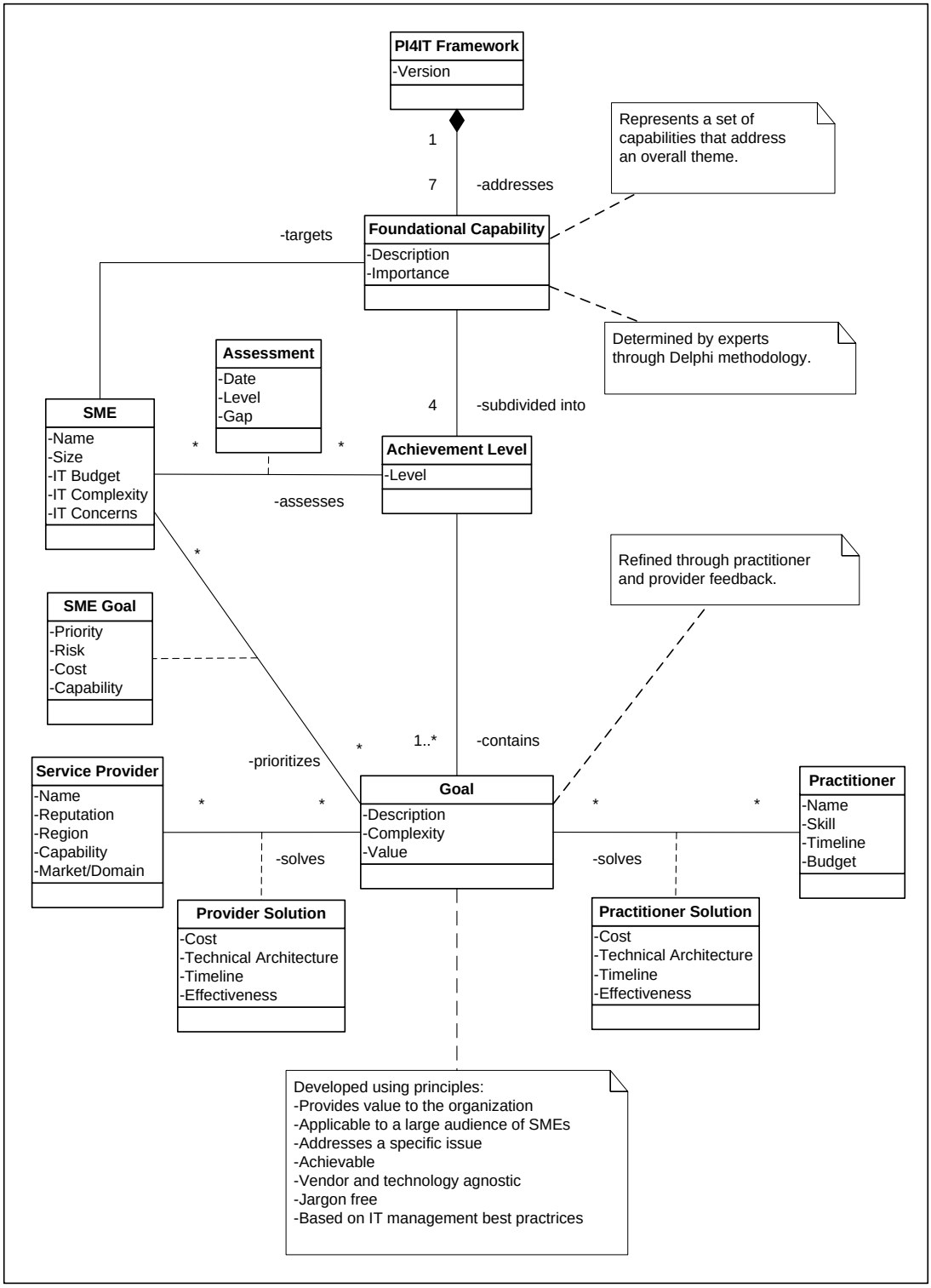
Sheskin, D. J. (2004). Handbook of Parametric and Nonparametric Statistical Procedures - Third Edition. Boca Raton: Chapman & Hall/CRC.

Silvius, G. (2004). IT and Small Business: An Unhappy Marriage. Innovations through information technology: 2004 Information Resources Management Association International Conference (pp. 316-318). New Orleans: Idea Group Inc.

Tarabishy, A. E. (2007). IT Issues. NFIB National Small Business Poll , 1-23.

ISSN: 2167-1508
v6 n2815

Appendix A: PI4IT Meta Model



Appendix B: PI4IT Quick Assessment Checklist

Instructions

1) This document is the quick assessment checklist for the different IT management categories of the PI4IT framework. Each category is broken down into four achievement levels. (See http://www.pi4it.com for full descriptions of each category)
2) Many of the goals will require knowledge of your IT management practices and thus is best completed with the assistance of or by the person who is considered the IT manager.
3) Choose the IT management category(ies) that you would like to assess and improve.
4) Start from the top most goal and check the Y (Yes) box if that goal is accomplished, N (No) if that goal is yet to be accomplished or U (Unsure) if you are unsure. Make notes at the bottom.
5) If a goal is not applicable to your environment then you can skip it.
6) Identify any Unsure answers and ask your IT advisor if the answer should be Yes or No as appropriate.
7) Evaluate all the No goals and assign them a priority based on business alignment, IT strategy, resources required, etc.
8) Improve your IT management performance by completing projects to accomplish remaining goals.

Notes

1) PI4IT's goals are technology independent. For example, one goal of the Backup category is to have an automated backup system. This goal can be accomplished whether you use Windows, Macintosh or Unix or whether you store data on tape, CD, flash drive, removable hard drive, or over the Internet.
2) It is perfectly acceptable to skip categories based on personal preference but you will find that many of the categories are complimentary. For example, to complete all the Disaster Recovery category goals you will complete several goals in the Backup category too.
3) PI4IT is updated often. You can download the latest quick assessment checklist at http://www.pi4it.com

Category	Level	Yes/No/ Unsure	Goals
Backup	1	OY ON OU	Identify important data that should be backed up.
		OY ON OU	Backups are performed manually or automatically.
	2	OY ON OU	Backups are performed automatically.
		OY ON OU	Occasionally test a data restore.
		OY ON OU	Document the backup and restore process.
	3	OY ON OU	Enable backup integrity options (i.e. verify the tape) as part of the automated backup scheme.
		OY ON OU	Enable status notification via e-mail or other means after every backup event.
		OY ON OU	Store backups in a remote location.
	4	OY ON OU	Perform a yearly data restore test for mission critical applications.

Category	Level	Yes/No/ Unsure	Goals
Disaster Recovery	1	OY ON OU	Determine how long the business can continue to function without critical IT systems.
		OY ON OU	Determine how far back in time the IT systems can be restored without significant inconvenience to the business.
		OY ON OU	Determine the system recovery priority/order (some systems may rely on others to operate).
	2	OY ON OU	Ensure insurance coverage exists for replacement value of IT assets.
		OY ON OU	Document the contact information for all key personnel.
		OY ON OU	Establish a secondary location (i.e. IT service provider or even someone's house) to recover services in the event of a major disaster at the primary site.
	3	OY ON OU	Detail key activities required for recovery of each IT system.
		OY ON OU	Specify what determines a disaster, when the plan should be enacted, and who can declare the disaster.
		OY ON OU	Assign recovery roles and responsibilities to team members.
		OY ON OU	Establish a backup power source (i.e. generator) to run key servers and workstations during temporary power loss events.
	4	OY ON OU	Perform a complete IT disaster recovery test annually for mission-critical systems.
		OY ON OU	Update the disaster recovery plan with every major change to the IT environment.

Category	Level	Yes/No/ Unsure	Goals
Hardware	1	OY ON OU	Build a thorough hardware inventory including hardware specifications, make, model, serial number and warranty expiration date.
		OY ON OU	Ensure that all broken hardware used for business purposes is repaired (or replaced).
	2	OY ON OU	Compare hardware specifications with software requirements. Upgrade or replace any hardware that does not meet the minimum software requirements.
		OY ON OU	Determine which applications are mission critical and what hardware is required to operate those applications.
		OY ON OU	Choose a company standard for hardware to minimize support costs and supplies (i.e. a choose a standard laser printer to reduce the different types of toner cartridges)
	3	OY ON OU	Monitor key systems for performance and availability metrics.
		OY ON OU	Purchase or upgrade hardware warranty contracts based on business requirements for acceptable downtime due to hardware repair.
		OY ON OU	Use RAID (redundant hard drive) technology on all servers.
		OY ON OU	Install Uninterruptible Power Supply (UPS) systems on all key systems (i.e. servers, network equipment, etc.)
		OY ON OU	Upgrade or replace hardware that does not meet recommended software requirements.
	4	OY ON OU	Analyze logs and monitor systems to determine performance-based or availability-based trends. Fix any issues that can cause business disruptions (i.e. hard drives are filling up).
		OY ON OU	Use redundant power supplies on all mission critical servers.
		OY ON OU	Use redundant network connections on all mission critical servers.

Category	Level	Yes/No/ Unsure	Goals
IT Strategy	1	OY ON OU	Determine how IT contributes to the success of the company.
		OY ON OU	Document the company's IT principles (Google "IT principles" for examples).
		OY ON OU	List all IT systems and categorize them as mission critical or non-mission critical.
		OY ON OU	List all IT services and categorize them as in-house or out-sourced (i.e. e-mail, help desk, accounting, etc.)
		OY ON OU	Identify any relevant industry compliance issues (safety, health, ergonomic, privacy, legal, regulatory, intellectual property, etc.)
	2	OY ON OU	Execute non-disclosure statements with all IT service providers that have access to business information.
		OY ON OU	Create a budget of annual IT expenditures.
		OY ON OU	Ensure that essential IT tasks are documented and known by more than one person.
		OY ON OU	Implement a change management process whereby all the major changes to the IT environment are summarized and dated in a change management log. Attach detailed information to the change log.
	3	OY ON OU	Develop and implement reasonable policies (such as an Acceptable Use Policy).
		OY ON OU	Manage IT projects by documenting what needs to be achieved, by whom, when, at what cost and with what benefits.
		OY ON OU	Evaluate your peers to determine how IT adds value to their organizations.
		OY ON OU	Develop an action plan for how to deal with the loss or termination of IT employees or IT service companies.
	4	OY ON OU	Create a written IT Strategic Plan (ITSP).
		OY ON OU	Review and update the ITSP annually.
		OY ON OU	Find opportunities for competitive advantage using IT.

Category	Level	Yes/No/ Unsure	Goals
Networking and Internet Technologies	1	OY ON OU	Network PCs to share Internet access (wired or wireless).
		OY ON OU	Establish e-mail accounts for employees.
	2	OY ON OU	Share files among users.
		OY ON OU	Share printer(s) among users.
		OY ON OU	Secure wireless networks by enabling encryption on access points (WPA2 or better is preferred).
		OY ON OU	Enable multi-user access to major business applications.
	3	OY ON OU	Establish virtual private networks to remote offices.
		OY ON OU	Monitor network availability.
		OY ON OU	Establish a domain name (.com etc.) and receive e-mail at that domain name.
		OY ON OU	Establish an e-mail SPAM (unsolicited bulk e-mail) filter.
	4	OY ON OU	Enable remote access to the network to access applications.
		OY ON OU	Enable remote access to the network to access shared files.
		OY ON OU	Implement measures to protect PCs from Internet attacks (i.e. firewall, intrusion protection, and tiered layers/DMZ).
		OY ON OU	Monitor Internet usage for unacceptable types of activity per company policy (i.e. inappropriate web sites and games).
		OY ON OU	Establish a web site using your domain name.

Category	Level	Yes/No/ Unsure	Goals
Security	1	OY ON OU	Obtain and read any security best practice documents for key business applications.
		OY ON OU	Obtain and read any security best practice documents for networking devices.
		OY ON OU	Determine the importance of the security of business data.
		OY ON OU	Determine which applications support security.
		OY ON OU	Determine if any form of security is enabled to access shared files.
		OY ON OU	Determine any physical security risks (i.e. backup tapes laying on desks, unlocked server rooms, etc.)
	2	OY ON OU	Compare security best practices for key business applications. Mitigate any unacceptable security risks.
		OY ON OU	Compare security best practices for networking devices. Mitigate any unacceptable security risks.
		OY ON OU	Establish a company security policy.
		OY ON OU	Restrict physical access to important business equipment and backups.
		OY ON OU	Establish unique accounts with passwords for each employee to access applications and shared data.
		OY ON OU	Restrict shared file access to only those who should have access.
		OY ON OU	Establish complex passwords for any administrator-level accounts.
		OY ON OU	Install Anti-virus protection on all systems and have it auto-update and scan regularly.
	3	OY ON OU	Enable screen savers on all systems. Require a password to resume the session. Set the wait/idle time to a reasonable value.
		OY ON OU	Enable scheduled password changes on systems.
		OY ON OU	Apply security-related patches (OS or application) regularly.
		OY ON OU	Review accounts on all systems at least yearly and disable/delete any unnecessary accounts.
		OY ON OU	Review and update (as necessary) the security settings on all shared files and network shares at least yearly.

		OY ON OU	Establish a firewall between the internal network and Internet that denies all non-approved inbound Internet communication.
		OY ON OU	Enable firewall protection on all hosts.
	4	OY ON OU	Audit all systems at least yearly using security tools. Actively mitigate vulnerabilities that are ranked medium or high risk.
		OY ON OU	Remove unnecessary applications or services from servers and workstations.
		OY ON OU	Perform company-wide annual security awareness and policy training.

Category	Level	Yes/No/ Unsure	Goals
Software	1	OY ON OU	Build an inventory of all the software in the environment. Include in the inventory the version, license keys, location of the installation media, number of installation licenses, number of purchased licenses, maintenance/service expiration date, annual maintenance cost, and the latest version number.
		OY ON OU	Address licensing issues (i.e. purchase missing licenses or uninstall unlicensed software).
	2	OY ON OU	Compare hardware specifications with software requirements. Upgrade or replace any hardware that does not meet the minimum software requirements.
		OY ON OU	Evaluate the software inventory and determine which application software has newer versions. Review the benefits and costs of the newer software. Determine how long the current version is supported. Make a decision to upgrade based on business requirements and risk.
		OY ON OU	Subscribe to vendor software update notification services.
		OY ON OU	Apply all security updates to software (OS or application) that are considered high risk.
	3	OY ON OU	Identify opportunities for automation such as OS updates for security patches or scheduled batch jobs. Automate tasks as appropriate.
		OY ON OU	Evaluate key software as to its effectiveness, efficiency and economics.
		OY ON OU	Document standard maintenance procedures for applications and application interfaces (i.e. batch jobs).
	4	OY ON OU	New applications or updates are tested on non-live systems before release.
		OY ON OU	New applications or updates are tested and accepted by end users.
		OY ON OU	Define service level agreements with third party application providers.