Continuous IT System Auditing

By

Leon J. Walker

A Thesis Submitted to the Faculty of the

DEPARTMENT OF MANAGEMENT INFORMATION SYSTEMS

ELLER COLLEGE OF MANAGEMENT

In Partial Fulfillment of the Requirements

For the Degree of

MASTER OF SCIENCE

In the Graduate College

THE UNIVERSITY OF ARIZONA

2015

STATEMENT BY AUTHOR

This thesis has been submitted in partial fulfillment of requirements for an advanced degree at the University of Arizona and is deposited in the University Library to be made available to borrowers under rules of the Library.

Brief quotations from this thesis are allowable without special permission, provided that an accurate acknowledgement of the source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part may be granted by the head of the major department or the Dean of the Graduate College when in his or her judgment the proposed use of the material is in the interests of scholarship. In all other instances, however, permission must be obtained from the author.

SIGNED: Leon J. Walker

APPROVAL BY THESIS DIRECTOR

This thesis has been approved on the date shown below:

____________________________________ 5/13/2015

Dr. Mark Patton Date

Professor of Management Information Systems

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Continuous auditing systems are designed to provide real-time assurance on the quality and credibility of information. The adoption of continuous auditing systems is typically driven by regulation, industry, and cost. Continuous auditing systems help by reducing the amount of field work involved and reducing the number of repetitive tasks an auditor needs to perform. Even though industry is being driven toward continuous auditing systems, not all systems are integrated within the organization at the same level. Continuous systems offer many benefits and can increase security, decrease inefficiencies, and reduce errors. However, the returns from the benefits seem to be tied to the amount of planning and re-engineering an organization is willing to commit to. This survey paper covers the multiple dimensions of continuous auditing systems while filling in weaknesses in previous works, concluding with a discussion on the viability of automating controls.

1 Introduction / Background

1.1 General Discussion of System Auditing

Continuous IT systems auditing can be broken into two parts. The first is the IT systems audit and the second the continuous audit. According to Davis (2011) the goal of an IT systems auditor is to improve the controls at a company while still helping the company or department meet its mission. Continuous auditing is, according to the CICA/AICPA (1999), "a methodology that enables independent auditors to provide written assurance on a subject matter using a series of auditors' reports issued simultaneously with, or a short time after, the occurrence of events underlying the subject matter". By combining these two definitions we can obtain our definition of continuous IT systems auditing.

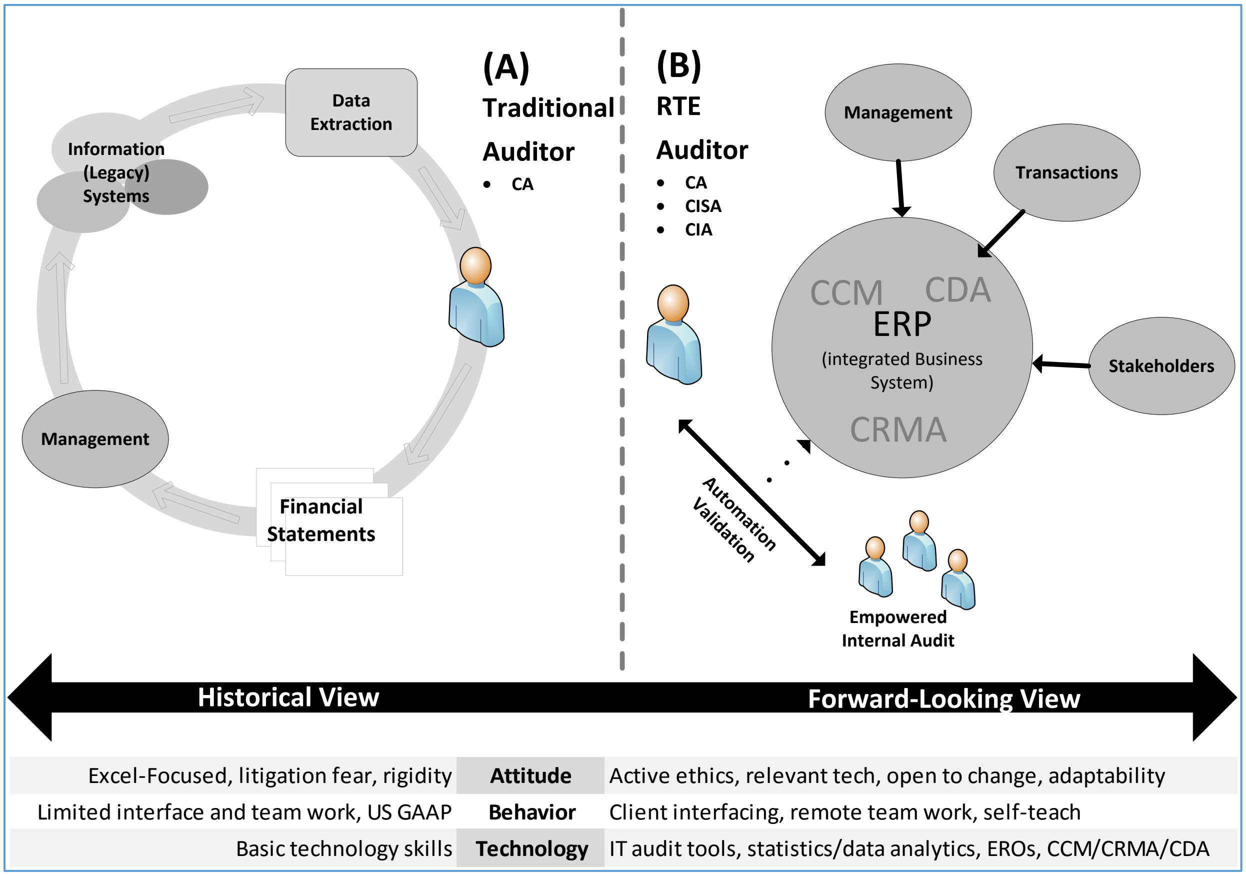
> Continuous IT system auditing is a methodology that helps a company or department meet its mission through enabling independent auditors to improve the controls at a company, by providing written assurance on a subject matter using a series of auditors' reports issued simultaneously with, or a short time after, the occurrence of events underlying the subject matter.

Continuous auditing is more than a compressed time frame for producing reports. A good comparison between traditional auditing and continuous auditing is provided by Chan (2011). As shown in Table 1 below.

Traditional auditing	**vs.**	**Continuous auditing**
1. Frequency: - Periodic	→	1. Frequency: - Continuous or more frequent
2. Approach: - Reactive	→	2. Approach: - Proactive
3. Procedures: - Manual	→	3. Procedures: - Automated
4. Work and role of auditors - Bulk of the work performed is centered around labor and time intensive audit procedures - Independent roles of the internal and external auditor	→	4. Work and role of auditors - Bulk of the work performed is centered around handling exceptions and audit procedures requiring human judgement - External auditor role becomes the certifier of the continuous auditing system
5. Nature, timing, and extent: - Testing consists of analytical review procedures and substantive details testing (nature) - Controls testing and detailed testing occur independently (timing) - Sampling in testing (extent)	→	5. Nature, timing, and extent: - Testing consist of continuous controls monitoring and continuous data assurance (nature) - Controls monitoring and detailed testing occur simultaneously (timing) - Whole population is considered in testing (extent)
6. Testing: - Humans perform testing	→	6. Testing: - Data modeling and data analytics are used for monitoring and testing
7. Reporting - Periodic	→	7. Reporting: - Continuous or more frequent

Table 1: Traditional auditing vs. continuous auditing methodology. (Chan, et al, 2011)

The frequency of audits is the first and most obvious difference between traditional auditing and continuous auditing. Continuous auditing systems change the approach to auditing. The automated procedures in system auditing creates a proactive approach allowing for the system to be monitored in real-time or on demand. Instead of waiting for an issue to be reported or waiting for a yearly audit to find issues, the continuous auditing system allows auditors to view a system's status at any time to look for issues. The increased frequency of audits is obvious, what is not is the effect of continuous auditing on the kind of work the auditor is doing, shown in Figure 1 below.



Excel-Focused, litigation fear, rigidity	**Attitude**	Active ethics, relevant tech, open to change, adaptability
Limited interface and team work, US GAAP	**Behavior**	Client interfacing, remote team work, self-teach
Basic technology skills	**Technology**	IT audit tools, statistics/data analytics, EROs, CCM/CRMA/CDA

Figure 1: Changing the Auditors Work (Vasarhelyi, et al, 2010)

Due to the automated procedures performing the tedious and repetitive tasks involved in auditing, the form of the auditor’s work is constantly changing. Auditors are now able to audit the whole extent of a system instead of sampling the most critical components. This improves the security of the audited system by creating an environment where no part of the system is overlooked. Automated systems with integrated auditing do not need to be stopped to perform tests. The testing of a system can be performed in real-time with the most current data available. Allowing for the system controls to be monitored continuously, which increases the assurance that the system is performing as expected and validates the integrity of the data provided by the system.

1.2 What is Continuous?

Continuous auditing and continuous monitoring seem to be very similar. The main point where these two systems differ is ownership. Continuous auditing systems are owned by the Information Assurance group or the auditors. Continuous monitoring systems are owned by management and IT. Both of these systems provide insights into risk and compliance, along with helping the organization perform efficiently and profitably (Verver, 2008). Since the output of the continuous auditing/monitoring system can be shared between owners, for the purpose of the rest of this paper they are considered the same.

Continuous monitoring does not require every system to monitor every transaction. National Institute of Standards and Technology (NIST) released a special publication SP 800-92 which provides guidelines (Table 2) on how often a system needs to be monitored.

CATEGORY	Low-Impact Systems	Moderate-Impact Systems	High-Impact Systems
How long to retain log data	1 to 2 weeks	1 to 3 months	3 to 12 months
How often to rotate logs	Optional (if performed, at least every week or every 25 MB)	Every 6 to 24 hours, or every 2 to 5 MB	Every 15 to 60 minutes, or every 0.5 to 1.0 MB
If the organization requires the system to transfer log data to the log management infrastructure, how frequently that should be done	Every 3 to 24 hours	Every 15 to 60 minutes	At least every 5 minutes
How often log data needs to be analyzed locally (through automated or manual means)	Every 1 to 7 days	Every 12 to 24 hours	At least 6 times a day
Whether log file integrity checking needs to be performed for rotated logs	Optional	Yes	Yes
Whether rotated logs need to be encrypted	Optional	Optional	Yes
Whether log data transfers to the log management infrastructure need to be encrypted or performed on a separate logging network	Optional	Yes, if feasible	Yes

Table 2: An example of recommend frequency for log management (Kent, et al, 2006)

The table separates systems based on the impact a breach would have on a particular system. The table NIST provides points out what it is to be a continuous auditing system. First log files are generated on a periodic basis. These log files are then uploaded to a log management system. Then an audit of the logs is performed on a less frequent basis compared to the generation of the logs. The frequency of the log generation, upload and audit are based on the risk of a breach. As a result systems are audited based on risk of breach, all systems can be part of continuous auditing. Knowing what potential risks face an industry and knowing how to manage the risks is import for knowing how frequently to monitor a system (Rezaee, et al, 2002). By breaking up the audit frequency based on risk, resources are freed up to handle the exceptions generated by the automated systems and to audit other systems.

2 Drivers: Regulation Compliance, Reducing Costs, and Industry Momentum

2.1 Regulation Compliance

The driving forces behind the move toward continuous auditing are regulation compliance, reducing auditing costs, and industry momentum. Maintaining compliance with regulation can be very time consuming and expensive. Continuous auditing helps business meet the demands of regulation compliance by reducing the amount of field work involved and reducing the number of repetitive tasks an auditor needs to perform (Vasarhelyi, 2012).

2.1.1 Sarbanes-Oxley Act (SOX)

SOX, also known as the Sarbanes-Oxley Act, passed in 2002 had a direct effect on the control practices of publicly traded companies. Ramamoorti (2004) points out three sections of SOX that have a specific impact on IT and continuous auditing: sections 302, 404, and 409. Section 302 requires the CEO and the CFO to sign off on the accuracy and completeness of financial statements. Section 404 affects the external auditors, requiring them to sign off on the effectiveness of internal controls effecting financial statements. Section 409 requires a company to rapidly report on financial position changes. The effects of the three SOX sections has been to require companies to create real-time reporting systems that are transparent, in that they provide a clear understanding of the underlying processes and controls (Ramamoorti, et al, 2004).

Companies want to automate SOX compliance. It was estimated that organizations that are part of the fortune 1000 will spend 2.5 billion as part of their initial compliance with SOX (Sodano, et al, 2003). Organizations are investing heavily in automating compliance because of the time and complications associated with a SOX audit. Those interviewed concerning continuous auditing and continuous monitoring reported that audit time was reduced and other review activities were better supported for SOX compliance (Vasarhelyi, et al 2012).

2.1.2 Federal Information Security Management Act (FISMA)

Where SOX is the driving regulation for publicly traded companies, FISMA is the regulation for government entities. FISMA requires every federal agency to implement an information security plan to protect agency assets and operations. This includes the operations and assets provided from outside sources (NIST, 2014). A requirement of FISMA is that systems must be continuously monitored based on the risk level a security breach would create, but all systems must be audited at least annually. Organizations are asked to monitor their systems in a way that effectively manages the risk to each system (NIST, 2010). The effect of FISMA is to require government agencies to implement continuous auditing systems that monitor the government systems on a risk based schedule.

Government regulation is not going away and will continue to have an effect on government IT operations. Research predicts that the most important support for regulation compliance will come from continuous auditing systems (Schultz, 2011). As a result of collecting the reports from continuous auditing systems, deeper information can be found such as trending data. The trending data will then provide feedback to improve compliance, operations, security, and risk posture. The trending data is likely to become an additional requirement for future government regulation (Schultz, 2011).

To meet the requirements of FISMA regulation some tools have been developed. An example of one such tool is CyberScope, which was introduced by the Department of Homeland Security (DHS). The CyberScope tool is intended to simplify the audit process by aggregating all the audit data onto a cloud based system instead of emailingall the documents. After the information is gathered it can then be reviewed by other supporting agencies. CyberScope was not adopted as quickly as was hoped due to issues like interoperability, correlation, and translation problems. These issues are being addressed by NIST's Security Content Automation Protocol (Schultz, 2011).

2.1.3 Gramm-Leach-Bliley Act (GLBA)

The GLBA is government regulation dealing with financial institutions. The goal of GLBA is to force financial institutions to protect customers' collected and stored data against security threats. NIST points out that log management through continuous auditing can be helpful in identifying and resolving security violations. (Kent, et al, 2006).

2.1.4 Health Insurance Portability and Accountability Act (HIPAA)

One of the first laws passed to protect consumers data is the 1996 legislation dealing with health care records, HIPAA. HIPAA protects consumer health data by requiring certain security standards to be met. The HIPAA security standards are explained by NIST in SP 800-66 part of which covers log management needs. The log management can be part of a greater continuous auditing system including regular reviews of log reports and document security and retention (Kent, et al, 2006).

2.2 Industry Momentum

2.2.1 Payment Card Industry Data Security Standard (PCI DSS)

An example of industry momentum toward continuous auditing is seen in the development of the PCI DSS. The major credit card players: Discover, Visa, MasterCard, American Express, and JCB (Japan Credit Bureau), combined efforts to create an additional level of security by ensuring vendor systems meet or exceeded a predefined level of security. The security focused on the protection of cardholder data while both at rest and in transit. (Williams, et al, 2014). In addition to protecting cardholder data all access to the data and the network resources it uses must be tracked (Kent, et al, 2006). The combined effort of the credit card companies became known as PCI compliance or PCI DSS. To meet the demands of compliance industries are moving to continuous auditing systems.

Regulation is enough to have the effect of driving a company to adopt a continuous auditing system. An example comes from the interviews done by Vasarhelyi (2012). In the paper, interviews were conducted with internal audit department managers. Some of these managers were not concerned with cost as a driver for the adoption of continuous auditing technology. The following question was posed to the executive management of the companies researched. "Is the main objective more of coverage than to less labor or costs?" A manager replied as follows.

> "…we want to use the computer more to audit than before… clearly if you can get both it is a win-win. Ultimately, the business auditors should be happier. Nobody likes to test 50 things over and over again."

A quick internet search shows that if a fine is less expensive than compliance with regulation, organizations will opt to pay the fine (Google, 2015). This behavior is seen in retail, entertainment, and even mining. Corporate behavior shows that even with regulation being such a strong driver for the adoption of continuous auditing systems there typically needs to be a cost advantage to implementing a continuous auditing system.

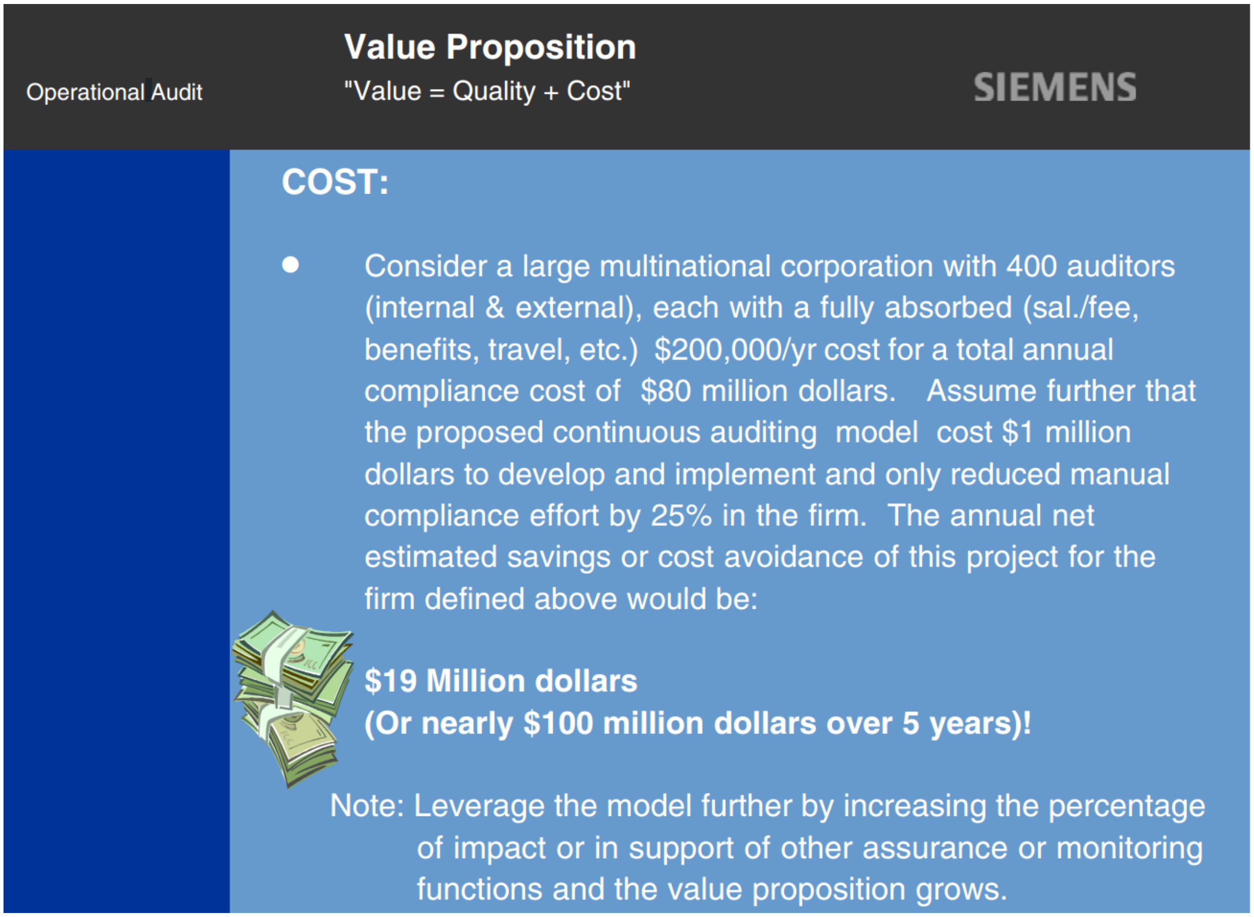
2.3 Cost

The costs associated with implementing continuous auditing systems is far from trivial. In six years the department of state spent about $133 million to be in compliance with FISMA. The US government as a whole is estimated to spend $2.3 billion per year on FISMA compliance as estimated by Tom Carper the Delaware Senator (Schultz, 2011).

In 2005, Siemens saw that implementing SOX would prove difficult with their current auditing process. Siemens has deeply integrated SAP (Systems, Applications and Products in Data Processing), enterprise resource planning software, into its systems. Each audit requires a large audit team to cover every SAP module and each audit would take almost 70 person days. Additionally there is the cost to fly the audit team to and from each audit site and the personal cost to each audit member. Due to the number of sites and the complexity of the systems being audited Siemens estimated that each site could be audited only once every two years. Putting them out of compliance with SOX. (Vasarhelyi, et al, 2012)

Siemens tasked their Information Assurance (IA) group to find a way to address the demands of SOX without increasing the employee count. The IA group's first goal was to understand the extent of which the current audit process could be automated. The initial estimation put the automated process at 25%. However, after becoming involved in the process they found that 68% of auditing actions could be automated. The increase in automated auditability was due to another of IA's goals, which is to enable continuous auditing by re-engineering the manual auditing process. With many of these processes moving from a two year audit cycle to automated daily audits. It was anticipated that a portion of the remaining 32% of audit processes would become unnecessary. The reason a portion of the 32% becomes unnecessary is because of the automated processes. The automated processes are not subject to interpretation from the auditor, and the automated process collects data more frequently and consistently providing stronger evidence (Vasarhelyi, et al, 2012).

As justification for the project Siemens internal audit team offered the following scenario which points out that the cost of implementing a continuous auditing system is far outweighed by the savings the system would provide. This example is shown in Figure 2 below.



Operational Audit

Value Proposition

"Value = Quality + Cost"

SIEMENS

COST:

- Consider a large multinational corporation with 400 auditors (internal & external), each with a fully absorbed (sal./fee, benefits, travel, etc.) $200,000/yr cost for a total annual compliance cost of $80 million dollars. Assume further that the proposed continuous auditing model cost $1 million dollars to develop and implement and only reduced manual compliance effort by 25% in the firm. The annual net estimated savings or cost avoidance of this project for the firm defined above would be:

$19 Million dollars
(Or nearly $100 million dollars over 5 years)!

Note: Leverage the model further by increasing the percentage of impact or in support of other assurance or monitoring functions and the value proposition grows.

Figure 2: Siemens Project Justification (Alles, et al, 2006)

If we look a little closer at the numbers and remember that Siemens was able to automate 68% of the auditing actions the savings become much larger.

System Cost	Labor savings	Compliance Savings	5 years
$ 1,000,000	68%	$ 53,400,000	$271,000,000

Table 3: Siemens at 68% automation

The Table above shows that if Siemens is realizing a 68% labor savings the investment into the continuous auditing system is saving them $53 million the first year and $271 million over the next five years. The Siemens example shows that implementing a continuous auditing system can be a significant cost advantage for a company.

If a system is re-engineered or developed around continuous monitoring, as part of the System Development Lifecycle (SDLC), additional cost savings are realized in application maintenance. If a system is designed to be as automated as possible, including the reporting requirements for regulation compliance, cost savings become almost inevitable. Systems like these could save the government and organizations thousands of labor hours spent on compliance. (Schultz, 2011)

Common controls are another way for organizations to reduce costs associated with continuous auditing. Common controls are shared security controls that provide outputs which are monitored by multiple owners. This makes it so each owner does not need to implement their own version of the control. The shared or common controls range from network boundary protection, and incident response, to physical security monitoring. As a result of making common controls available across an organization and sharing with many owners, common controls become a cost-effective way to implement information security. (NIST, 2010)

There are cost savings to implementing continuous auditing / continuous monitoring systems. To realize the greatest savings, organizations should re-engineer the auditing process with a focus on automation, design processes as part of the SDLC to reduce maintenance costs, ensure the automation of compliance reports, and leverage common controls. Organizations that develop continuous auditing in this way could see significant savings.

3 System Integration

3.1 Level of Adoption

Not all continuous auditing systems are integrated with the organization at the same level. Teeter and Brennan (2010) point out that this is due to auditors implementing auditing tools that provide a quick victory. This can include using tools built into existing systems or automating existing process that are highly repetitive and prone to automation. An example of this is found in the Vasarhelyi (2012) paper. One of the managers interviewed on continuous auditing had this to say about existing systems.

> "Our IT service colleague already has the tools that monitor the configurable settings for the systems, databases, and network. What we need to do is work with them to get them into where they are continuously monitoring. Then, our audit can focus on how we are going to deal with the exceptions. We've got to get them to implement that capability in order for us to be able to get out of the mode of writing scripts, etc."

Schultz (2011) also echoes this sentiment by pointing to the systems administrators who are using tools and applications to monitor systems, networks, and data. These tools help the administrator monitor system compliance and vulnerability. The tools used by the system administrators can be used as part of the continuous auditing system. This would provide common controls that can be used to increase real-time visibility for incident detection, incident response, and the state of system compliance. By managing the log files generated by these systems and looking for trends over time auditors would have a tool to manage risk, predict areas of improvement, and monitor the state of system security.

While evaluating a pilot program to transition IT audit to continuous control monitoring it was found that 50% of the controls need either no change or very little modification to work with the new system. It was further found that an additional fourth of those controls could also be re-engineered to become viable for auditing (Alles, et al, 2006). By leveraging the success of implementing the controls that need no modification, the benefits of continuous auditing can be shown. This prepares an organization to move onto the controls that need re-engineering to make continuous auditing more prevalent in the organization. Differing levels of continuous auditing adoption can be seen in Figure 3 below.

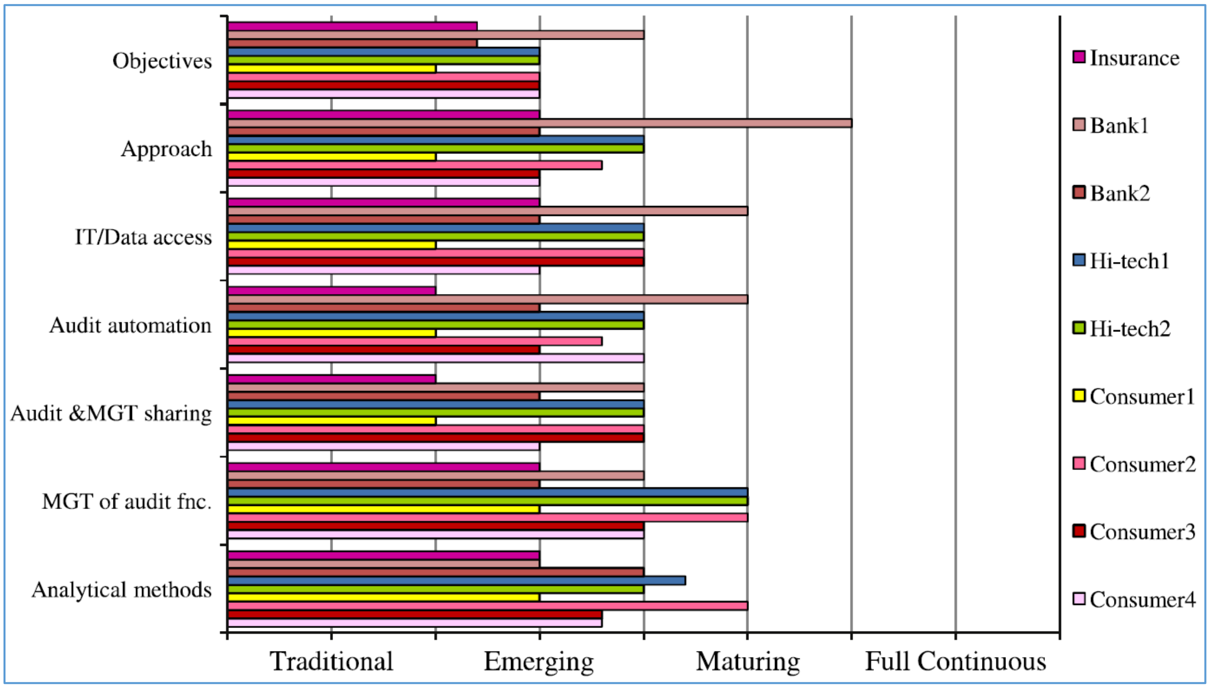
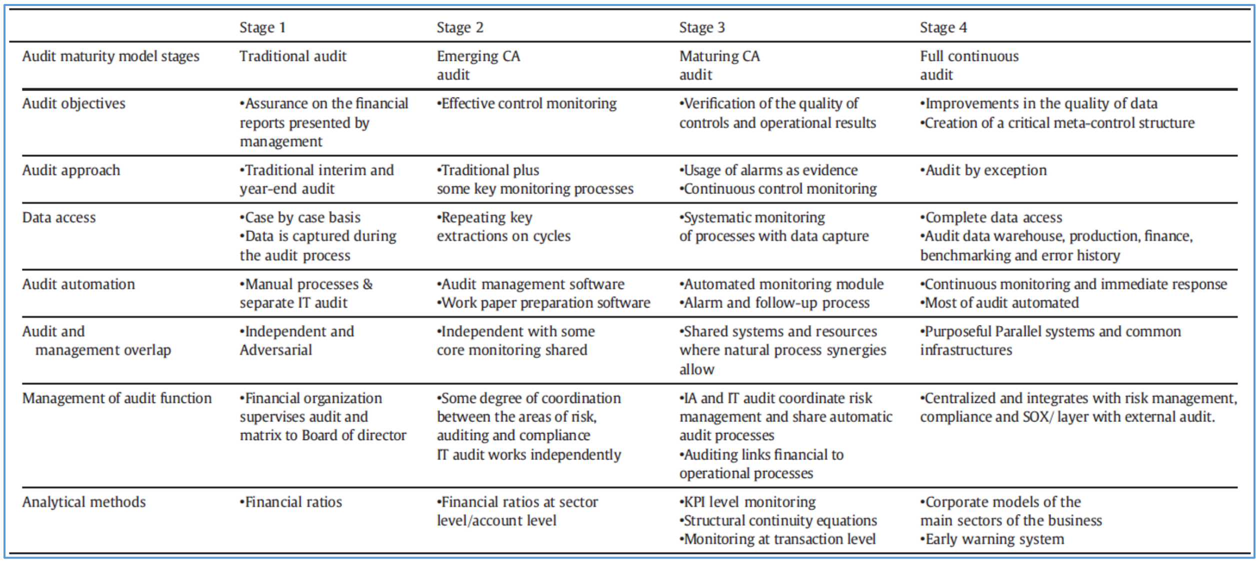


Figure 3: Adopted levels of continuous auditing maturity (Vasarhelyi, et al, 2012)

After capturing and implementing those controls that require little change to be used for continuous auditing, an organization may wonder what the next milestone is in continuous auditing adoption. This question can be answered in part by the Audit Maturity Model found in Table 4.



	Stage 1	Stage 2	Stage 3	Stage 4
Audit maturity model stages	Traditional audit	Emerging CA audit	Maturing CA audit	Full continuous audit
Audit objectives	•Assurance on the financial reports presented by management	•Effective control monitoring	•Verification of the quality of controls and operational results	•Improvements in the quality of data •Creation of a critical meta-control structure
Audit approach	•Traditional interim and year-end audit	•Traditional plus some key monitoring processes	•Usage of alarms as evidence •Continuous control monitoring	•Audit by exception
Data access	•Case by case basis •Data is captured during the audit process	•Repeating key extractions on cycles	•Systematic monitoring of processes with data capture	•Complete data access •Audit data warehouse, production, finance, benchmarking and error history
Audit automation	•Manual processes & separate IT audit	•Audit management software •Work paper preparation software	•Automated monitoring module •Alarm and follow-up process	•Continuous monitoring and immediate response •Most of audit automated
Audit and management overlap	•Independent and Adversarial	•Independent with some core monitoring shared	•Shared systems and resources where natural process synergies allow	•Purposeful Parallel systems and common infrastructures
Management of audit function	•Financial organization supervises audit and matrix to Board of director	•Some degree of coordination between the areas of risk, auditing and compliance IT audit works independently	•IA and IT audit coordinate risk management and share automatic audit processes •Auditing links financial to operational processes	•Centralized and integrates with risk management, compliance and SOX/ layer with external audit.
Analytical methods	•Financial ratios	•Financial ratios at sector level/account level	•KPI level monitoring •Structural continuity equations •Monitoring at transaction level	•Corporate models of the main sectors of the business •Early warning system

Table 4: Audit Maturity Model (Vasarhelyi, et al, 2012)

The Audit Maturity Model breaks organizations down into four groups by the level of continuous auditing adoption that has been implemented. Stage 1 represents organizations that have not implemented continuous auditing in anyway and are still doing auditing in the traditional fashion. Stage 2 are the organizations that have begun transitioning toward continuous auditing by implementing auditing controls that can be found in existing systems and processes that need no re-engineering. Stage 3 organizations have reviewed the auditing process and have re-engineered as many aspects of the audit as possible to be automated. Stage 4 organizations have taken the automated audit process and have created common controls from that process to support all aspects of the organization.

Not all organizations have the same maturity level. However, government regulation is pushing organizations to increase the level of maturity for continuous auditing. As a result of following steps of transitioning existing controls, re-engineering audit processes, and creating common controls organizations have a simple map to follow to further develop their continuous audit maturity level.

3.2 Benefits of Continuous Auditing.

There are many benefits to continuous auditing. Some of the benefits from earlier sections include compliance with government regulation, potential cost savings from reducing needed man-hours, compressed timeframe for creating audit reports, testing the whole data set instead of sampling, and changing the type of work auditors perform. However, there are less obvious benefits associated with continuous auditing.

Schultz (2011) points out several benefits of continuous auditing. It provides awareness of the change in risk factors over time which increases management's visibility allowing them to adapt by modifying risk governance. By monitoring the changes in risk, management is more likely to be aware of developing risk and take corrective action before it becomes excessive, too difficult, or expensive to manage. The monitoring of risk can be done through the use of a log management system. The log management system would collect and analyze the logs to help the organization to identify events that will have a significant impact as compared to events that would have a minimal impact. Continuous auditing and log management would provide real-time, or near real-time, risk management; providing management the vital information required to make decisions that are risk based, cost effective, and mission centric.

The increase of risk visibility is seen in the State Department's application of continuous auditing. The State Department estimates that by implementing continuous risk monitoring it will improve its risk posture by 90 percent (Rudman, 2010).

Another benefit of continuous auditing systems is situational awareness or knowing what is going on. Mica Endsley defines the term situational awareness in her 1995 paper as the following:

> “The perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future” (Endsley, 1995).

But situational awareness deals directly with the automation of systems. As systems do more and more and system operators do less and less and the operator is still responsible for understanding the system state. If thing goes wrong the operator needs to intervene (Sheridan, et al, 2006).

Continuous auditing systems are constantly monitoring controls, networks and systems. Because of continuous auditing systems, auditors and managers have an increased situational awareness of the monitored environment. This allows auditors to can act on the exceptions, errors, or predictions generated by the system.

Systems developed for continuous auditing help organizations by providing the auditor tools to increase the auditor’s efficiency. Continuous auditing tools allow for the benchmarking of controls so they can be compared over time or against other controls. This increases the efficiency of external audits since the tools provide what the auditors need. With the tools providing unbiased output the external auditors are able to rely on the internal auditors work. This decreases the time and effort spent on an audit by both external and internal auditors. Two managers had the following to say on the efficiency of the tools and the time saved.

> “…we developed out the tools that can dump everything out on the table… so much of our objective for this has been SOX and driven by [external auditor]” (Vasarhelyi, et al, 2012).

> "To the extent of last year 100% of all the testing that [external auditor] would have performed for SOX is performed by the company…They would rather get more efficient in terms of how they review...Then when it came time for SOX to come into play we needed to be more efficient in how we audit it" (Vasarhelyi, et al, 2012).

Fraud and error can be caught in real-time with continuous auditing systems. Under traditional auditing fraud and errors are usually found. However, the fraud or error is normally may be found long after they have occurred. The delay between action and discovery of fraud and errors can have a significant negative impact on an organization. Real-time discovery of fraud and errors can be achieved through the integration of continuous auditing systems with the organizations enterprise systems. Errors can be audited at the transaction level and by looking over time at a trending level. This provides a view of potential vulnerabilities in the system (Flowerday, et al, 2006).

Continuous auditing systems work at the speed of real-time business. Before the implementation of an automated system the auditor would make a request to the IT department and wait to have the request filled. An IA manager had the following to say about the process. "We had some challenges [with the IT organization to get data] but generally not. The biggest challenge really is the time it takes to get it." After the implementation of a continuous auditing system companies are able to automate the data extraction process and share the data without the need for IT to fill the requests. By automating the process the collected data maintained its confidentiality and integrity (Vasarhelyi, et al, 2012)

3.3 Planning

Planning is crucial to the development of continuous auditing systems. Traditional auditing is expensive in both labor and time. Due to these restrictions traditional auditing is often limited to an annual event (Vasarhelyi, et al, 2011). However, because of the high expense of time and labor in traditional auditing the focus is shifting from traditional manual methods to automated technology-based methods (Bierstaker et al., 2001).

Knowing the underlying systems that will be used in the continuous auditing system provides insight for the planning process. Some of the technologies that continuous auditing rely on are web application servers, web scripting solutions, database management systems, connectivity solutions, business intelligence software, data analysis software, and Enterprise Resource Planning (ERP) systems. By leveraging these other systems a continuous auditing system can meet its planed goals (Sarva, 2006).

Multiple departments need to be involved in the planning process of a continuous auditing system. Members from these departments will make up a team of varying technical skills and management levels. The team will help plan a program capable of identifying, quantifying, and reporting system control failures including duplicate records, payment violations, and policy or rule violations (Schultz, 2011).

Organizations who plan appropriately can look forward to the benefits of a quality continuous auditing system. However, NIST provides a warning for organizations who are unwilling to put sufficient effort into the planning process.

> “Organizations should exercise caution in focusing solely on continuous monitoring at the expense of a holistic, risk-based security life cycle approach.

> Without the appropriate planning for security controls (preferably early in the system development life cycle) and the correct implementation of those controls, the value of continuous monitoring is greatly diminished. This is because the near real-time, ongoing monitoring of weak and/or ineffective security controls resulting from flawed information security requirements can result in a false sense of security" (NIST, 2010).

If a continuous auditing system is not a carefully planned part of the SDLC it can do more than leave security gaps in the system, it can create a system that is unusable for the intended purpose. The requirements gathering portion of the SDLC can prove to be the most important activity in planning a continuous monitoring system, if it is done correctly. Doing requirements gathering correctly provides a clear understanding of the problem, the business needs, and how the new system should handle them. Requirements gathering also insures that the system development is not derailed and stays focused on the stated problem by providing an understanding of the organization's processes, goals, business needs, and limitations. To achieve the continuous auditing goals the functions for systems technical components and processes need to be defined. An example includes metrics for system uptime, functionality for system components currently running, and output latency (Schultz, 2011).

4 Research Gaps

Many of the papers written about continuous systems auditing are written from the view of financial auditors. This provides a good starting point for evaluating continuous auditing systems, but these papers often leave out areas of a whole IT system audit. These areas include, but are not limited to, security, accountability, and user management.

Failing to plan a system with security in mind can create systems that quickly fall out of the desired level of compliance. Parts of the system that need to be monitored with security in mind include network systems, applications, and end user systems. Failing to manage updates and patches is what can cause these systems to no longer meet compliance standards (Schultz, 2011).

There are controls that do not lend themselves toward automation. Therefore automation cannot be used effectively in monitoring those controls which include management controls, technical controls, and operational controls. Because of this organizations are cautioned against focusing only on continuous monitoring instead of a complete life cycle approach. If organizations focus only on automation they will develop some ineffective controls. These weak controls can create a false sense of security. Without correctly planning and designing controls early in the SDLC the value created by implementation of the controls is partially lost (NIST. 2010).

The writing of financial auditors leaves two questions for the continuous auditing planner. The first is where continuous auditing is possible and where is it improbable. And the second is what aspects of security, accountability, and user management need further consideration in the planning, development, and monitoring process.

4.1 Security

The security of data is important to every company. Rezaee (2002) glosses over the need to audit system security, claiming that the auditor needs to take a risk oriented approach in auditing internal controls that are performed by electronic testing of firewalls, authentication, passwords, and encryption. Chan (2011) also briefly mentions security as internal controls that are designed to notify an auditor of violations. Flowerday (2006) does a much better job at addressing security. Flowerday points out the following: “There is also a need to ensure the security of the system. A system which is not secure is not reliable.” At which point Flowerday directed the reader to standards on internal controls such as COBIT but does not comment further on security.

Securing a continuous auditing system is more complicated than first anticipated. A requirements analysis needs to be performed. The analysis will dictate how to secure each component of the system, the system environment, and the data collected. As an example a requirement would include that the monitoring controls be secured on a server, the server would be physically secured in a room that requires biometric authentication, or another form of strong authentication, to access the server (Schultz, 2011).

To meet the needs of a company an IT auditor makes sure the sensitive data and the systems that handle the sensitive data are protected. This can be done through a defense in depth or layered security model (NIST, 2010). An example of defense in depth would include security at multiple points in the whole system such as, but not limited to, the following:

- External router
- Firewall
- Internal router
- Switches
- System access control
- System firewall

- Application access control
- Managed user rights

Layered security prevents unauthorized access from external and internal sources by protecting data with multiple checks (Harris, 2012).

Once the layers of defense have been decided and the systems and processes that need monitoring have been identified it is time to decide how to respond to policy violation. The policy would dictate if an immediate action is taken such as notifying the auditor or if the system takes action itself. If an account fails to login after an attempt or two it is not likely to be a serious threat. However, some actions do pose a serious threat and should generate a near real-time report that is coordinated with additional systems. Examples include attempted modification to the kernel, changes to applications, and privilege escalation (Schultz, 2011).

Many aspects of a layered security system can be automated. An aspect list may include but is not limited to the network equipment. Routers, firewalls, switches, can have their configurations downloaded and compared to baseline configuration. If a part of the system does not meet the configuration standard a notice can be sent to the auditor and the network manager. The possibility of automating is shown through the use of scripts to audit systems. Davis (2011) points out repeatedly that using tools, such as scripts, to increase the speed of the audit while maintaining audit validity is to the benefit of the auditor and the company. This would ensure that the network equipment is configured as expected. As an automated process this check could be run on demand or at specified intervals adding increased security against attacks.

Dempsey (2011) says that data is stored and transmitted across many different systems within an organization. When addressing sensitive data it needs to be secure while at rest and while in transit as part of data management. A way to do this is to develop a Data Loss Prevention (DLP) strategy.

This strategy deals with the monitoring, collection, use, storage, transmission, classification and disposal of data while at rest or in transit.

There are checklists and best practice standards that can help in auditing and designing a system. While an externally generated checklist is not likely to be fully comprehensive of an organization's internal system, they do provide a good place to start discussion and brainstorming on how to audit and secure a system (Davis, et al, 2011). An example of a simple checklist on application security is shown in Table 5 below.

Application Best Practices	
□	Apply defense in depth
□	Use a positive security model
□	Fail safely
□	Run with least privilege
□	Avoid security by obscurity
□	Keep security simple
□	Detect intrusions and keep logs
□	Never trust external infrastructure and services
□	Establish secure defaults
□	Use open standards

Table 5: Application Best Practices (Davis, et al, 2011)

4.2 Accountability

Continuous auditing produces more complete audit coverage. This coverage should increase the organizations governance by improving accountability and monitoring of transactions and reporting. In addition continuous auditing reduces audit costs while increasing the effectiveness of the audit. (Ramamoorti, 2004)

The idea behind accountability is that when something goes wrong there is an identified entity with responsibility to resolve the issue. Continuous audits keep users accountable for their actions. Continuous auditing provides a tools that can track individual behavior on the system, catch intrusions, and through logs provide legal evidence if necessary (Harris, 2012).

Another aspect of accountability is the separation of duties. Allowing the administrator responsibility for the system that gathers log data and also giving that administrator the responsibility to review the logs provides the opportunity to manipulate the data. A better option, when it comes to log management, is to have log administrators who verify the work of the system administrators. By having an objective party review the logs the system administrator is held accountable for their actions. This includes ensuring system logging is enabled. The separation of duties can be accomplished by storing log data on a server that is different from the system that created the logs. This allows the log administrator to maintain controls of the logs while denying access to the system administrator (Kent, 2006).

4.3 User Management

User management encompasses approving or denying user access on an organization's systems (Harris, 2012). User management includes the hiring and termination process, password management, system rights, change management, and group and policy management.

The hiring and termination process dictate the treatment of user accounts at the beginning and end of employment. This process is important, it manages the return of an organizations property and takes steps to prevent an unhappy employee from abusing privileges and comprising systems. Administrators are responsible to create accounts for legitimate business purposes. Failing to do so could place the integrity of organization’s systems at risk. A continuous auditing system could help maintain system integrity by performing the following tasks:

- Verifying the legitimacy of account requests
- Automatically suspending accounts during extended leave or termination
- Manage network access rights based on position
- Modifying access during a position change
- Validating active accounts against active employees

Automating these processes would help ensure the integrity of a system. However, user password management prevents unauthorized access as well. If a password is easy to guess it can allow for a system to be compromised by a malicious entity. Weak passwords are vulnerable to multiple types of attacks including guessing, brute force, and dictionary attacks. To help prevent this a continuous auditing system can provide assurance that the passwords are strong by enforcing an organization’s password policy (Davis, 2011).

4.4 Automation

Before processes are automated they must be formalized. Often audit process are adopted from legacy procedures for traditional manual audits. This creates approved audit programs that lack formalization. The lack of formalization creates issues in that it allows auditors to interpret audit programs differently (Alles, et al, 2006).

> “Since manual audit programs were not designed for automation, formalisable and judgmental procedures are often intermixed. To formalize and automate such a program, a redesign is usually required to separate out formalisable and automatable audit procedures from the others. Such a redesign amounts to re-

> engineering the audit program and should be done systematically (as opposed to ad-hoc) and based on the top-down analysis of enterprise risks to make sure that the redesigned procedures appropriately address all exposure areas" (Vasarhelyi, et al, 2010).

There are many controls that do lend themselves to automation. In the NIST Special Publication 800-53 there are security controls that meet this description. Examples include access control, authentication, and identification, accountability, and communication protection. These technical controls are all quality options to begin automation (NIST, 2010). Once auditing processes are formalized organizations are able to identify which controls can be implemented quickly, which controls need to be re-engineered before implementation, and which controls cannot be automated.

4.4.1 Exercise Evaluating Examples of Entity-Level Controls

In this section a quick evaluation of three entity level controls will be performed. The goal of the evaluation is to identify if the control can be automated, and to what degree should the control be automated with reason behind the decision. The exercise is a priori in practice and all decisions are proposals not definitive on previous research or works.

Entity-level controls, are controls that are pervasive through the entire business entity. Entity level controls are important to check first since these controls can be checked once and considered audited if the control appears in other smaller scope audits. Automating the auditing of any entity-level controls could provide significant time savings (Davis, et al, 2011).

1. Review of the IT Organization Structure for Assignment of Authority and Responsibility

This control would be a manual process and not prone to automation. This is due to reporting structures varying greatly between each organization. Because of the variations no standardization or off the shelf software to cover auditing of reporting structures is available. That leaves the option of creating a custom piece of software in house. The time and cost required to program a system to understand a reporting structure is greater than the time and cost to review manually. This should be a quick manual process and the cost to automate is not viable for the perceived return.

2. Review IT Strategic Planning Process

This control could be partially automated. The part of the control that cannot be automated is the planning part. Computers don't understand plans or intents. It is improbable to program a computer to develop and propose a plan. However, a system can be automated to track the metrics of the plan which would then monitor any deviations and report on the changes. In addition a digital record of plan sign offs should be kept. This would allow for tractability and accountably of the planning process.

3. Review Key Performance Indicator (KPI) and Process Metrics

This control can and should be one of the first to be automated, since this control has high visibility toward management. By definition a KPI is a measurable value and KPIs are significant enough to warrant constant monitoring. KPIs can be tied to a dashboard for quick review by management and auditing personnel. Examples of KPIs include System up time, mean time to repair, compare goal budget to actual budget, and income.

This exercise shows that not all controls can be automated. By dedicating time to planning and the willingness to re-engineer processes, the number of automated controls will increase. But the goal of automation should never take precedence over creating a system with a holistic security life cycle approach.

5 CONCLUSION

In summary, this paper has provided a deeper understating of continuous auditing systems. They are complex systems that integrate with every level of an organization and their processes. By examining recommendations for monitoring, continuous becomes a risk based time value instead of a constant stream tracking every interaction. As a result, continuous auditing becomes less resource intensive than what may be perceived.

The adoption of continuous systems is accelerated, if not almost mandated, by the need to meet with government regulation compliance. This is seen in the mandates for system reviews to be conducted in a timely fashion instead of bi-yearly or on a random basis. Fortunately by meeting compliance standards, through the implementation of a continuous auditing system, the cost and time needed to preform audits is greatly reduced.

Often when developing a system security is overlooked or it is assumed that current security controls are enough. The need to produce a system in a short time frame with high performance mistreats the need for security. An organization cannot focus on automation alone, doing so develops controls that are weak creating vulnerabilities in the system. By discussing security with the other aspects that effect continuous auditing such as user management, separation of duties, defense in depth, and accountability, a comprehensive system is reviewed.

6 REFERENCES

Alles, M., Brennan, G., Kogan, A., & Vasarhelyi, M. A. (2006). Continuous monitoring of business process controls: A pilot implementation of a continuous auditing system at Siemens. International Journal of Accounting Information Systems, 7(2), 137-161.

Bierstaker, J. L., Burnaby, P., & Thibodeau, J. (2001). The impact of information technology on the audit process: an assessment of the state of the art and implications for the future. Managerial Auditing Journal, 16(3), 159-164.

Chan, D. Y., & Vasarhelyi, M. A. (2011). Innovation and practice of continuous auditing. International Journal of Accounting Information Systems, 12(2), 152-160.

Davis, Chris (Christopher Michael) & Schiller, Mike & Wheeler, Kevin (2011). IT auditing: using controls to protect information assets (2nd ed). McGraw-Hill, New York

Dempsey, K., Chawla, N. S., Johnson, A., Johnston, R., Jones, A. C., Orebaugh, A., ... & Stine, K. (2012). Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations: National Institute of Standards and Technology Special Publication 800-137..

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. Human Factors: The Journal of the Human Factors and Ergonomics Society, 37(1), 32-64.

Flowerday, S., Blundell, A. W., & Von Solms, R. (2006). Continuous auditing technologies and models: A discussion. Computers & Security, 25(5), 325-331. doi:10.1016/j.cose.2006.06.004

Google. (n.d.). Retrieved May 8, 2015, from https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1GIGM_enUS540US540&ion=1&espv=2&es_th=1&ie=UTF-8#safe=off&q=company pays fine instead of fixing violation

Harris, S. (2012). CISSP exam guide (6th ed.). Berkeley, CA: Osborne ;.

Kent, K., & Souppaya, M. (2006). Guide to computer security log management. NIST special publication, 92.

NIST. (2010, June 1). FREQUENTLY ASKED QUESTIONS Continuous Monitoring. Retrieved May 4, 2015, from http://csrc.nist.gov/groups/SMA/fisma/documents/faq-continuous-monitoring.pdf

NIST. (2014, April 1). Detailed Overview. Retrieved May 3, 2015, from http://csrc.nist.gov/groups/SMA/fisma/overview.html

Ramamoorti, S., & Weidenmier, M. (2004). The pervasive impact of information technology on internal auditing. Supplemental chapter for Research Opportunities in Internal Auditing, edited by A. Bailey, A. Gramling, and S. Ramamoorti. Altamonte Springs, FL: IIA Research Foundation.

Rezaee, Z., Sharbatoghlie, A., Elam, R., & McMickle, P. L. (2002). Continuous auditing: Building automated auditing capability.Auditing, 21(1), 147-163.

Rudman, D. (2010, May 1). Enterprise Network Management iPost: Implementing Continuous Risk Monitoring at the Department of State. Retrieved May 8, 2015, from http://www.state.gov/documents/organization/156865.pdf

Sarva, S. (2006). Continuous auditing through leveraging technology. Information Systems Control Journal, 2, 47.

Schultz, E. (2011, June 1). Continuous Monitoring: What It Is, Why It Is Needed, and How to Use It. Retrieved May 4, 2015, from https://www.sans.org/reading-room/whitepapers/analyst/continuous-monitoring-is-needed-35030

Sheridan, T., & Parasuraman, R. (2006). Human-automation interaction: Taxonomies and Qualitative Models. In R. S. Nickerson (Ed.), Reviews of human factors and ergonomics (Vol. 1, pp. 89–129). Santa Monica, CA: Human Factors and Ergonomics Society.

Sodano, L., and J. Hagerty. (2003) Prioritizing IT Investments for Sarbanes-Oxley Compliance: AMR Research.

Vasarhelyi, M. A., Alles, M., Kuenkaikaew, S., & Littley, J. (2012). The acceptance and adoption of continuous auditing by internal auditors: A micro analysis. International Journal of Accounting Information Systems, 13(3), 267-281.

Vasarhelyi, M., Alles, M., & Williams, K. (2010). Continuous Assurance for the Now Economy. A Thought Leadership Paper for the Institute of Chartered Accountants in Australia.

Verver, J. (2008). Continuous Monitoring and Auditing: What is the difference?. Protiviti's KnowledgeLeader.

Williams, B. R., & Chuvakin, A. (2014). PCI compliance: understand and implement effective PCI data security standard compliance. Syngress.

7 Acronyms List

IT	Information Technology
CICA	Certified Internal Controls Auditor
AICPA	American Institute of Certified Public Accountants
ERP	Enterprise Resource Planning
CCM	Continuous Controls Monitoring
CRMA	Continuous Risk Monitoring and Assessment
CDA	Continuous Data Auditing
US GAAP	United States Generally Accepted Accounting Principles
CA	Certified Accountant
CISA	Certified Information Systems Auditor
CIA	Certified Internal Auditor
NIST	National Institute of Standards and Technology
SOX	Sarbanes-Oxley Act
CEO	Chief Executive Officer
CFO	Chief Financial Officer
FISMA	Federal Information Security Management Act
DHS	Department of Homeland Security

GLBA	Gramm-Leach-Bliley Act
HIPAA	Health Insurance Portability and Accountability Act
PCI DSS	Payment Card Industry Data Security Standard
SAP	Systems, Applications and Products in Data Processing
IA	Information Assurance
SDLC	Software Development Life Cycle
COBIT	Control Objectives for Information and Related Technology
DLP	Data Loss Prevention
KPI	Key Performance Indicator