JOURNAL OF EMERGING TECHNOLOGIES IN ACCOUNTING
Vol. 14, No. 1
Spring 2017
pp. 1–12

American Accounting Association
DOI: 10.2308/jeta-10539

EDITORIAL

Cybersecurity and Continuous Assurance

INTRODUCTION

The AICPA is issuing its cybersecurity guide in response to the need for involvement by the audit profession in the progressive evolution of cyber threats. This is seriously affecting the risk assessment process, which has become an even more important part of the audit process (AICPA 2016). This paper addresses the most pressing topics in cybersecurity: the need for new approaches for its assurance. In this paper, we argue that the traditional audit model, developed for the era of brick-and-mortar business, does not properly fit into the development of the smooth aggregation of assurance services that should exist in the arena of progressively automated multiple assurance processes. These processes are an essential part of the future corporate ecosystem. In particular, at least three basic elements of the traditional audit model need to be reconsidered: (1) the point-in-time report, (2) the zero/one nature of an opinion,[1] and (3) the concept of a fair representation threshold (materiality). These elements are intrinsic to a different age, a different technology, and different needs of investors and other corporate stakeholders.

A Different Time

The evolution of the double entry accounting model (Pacioli 1494; Sangster 2016) was based on the business practices of Venetian traders at the time, and focused on physical assets as well as debt including credit. The operations of many businesses were run on transaction records and accounting to secondary owners using those records. In the United States, the Great Depression motivated the Securities Exchange Act of 1934, which requires publicly traded companies to file their financial reports based on Generally Accepted Accounting Principles (GAAP) with the Securities and Exchange Commission (SEC). These reports are accompanied by an attestation of fair representation by independent auditors. Early market studies (e.g., Ball and Brown 1968) found a high relationship between stock market valuation and accounting values. Five decades later, Lev (1989) reported that adjusted R^2s find that accounting variables explain substantially less of corporate market values. Lev (1989) argues that traditional financial variables need to be supplemented by nonfinancial variables such as the value of human resources, intellectual property, supply chain, and brand. A substantive body of literature has evolved arguing for expanded reporting that includes these measures, and even the incorporation of sustainability measures (e.g., integrated reporting—Eccles and Krzus [2010]; sustainability reporting—Schaltegger, Bennett, and Burritt [2006]). Furthermore, organizations now run their businesses with a plethora of data drawn from their Enterprise Resource Planning (ERP) systems. This creates an environment where traditional financial numbers are mainly used for corporate compliance and not management decision making. Consequently, the assurance of traditional numbers that are not being actively utilized in corporate management and progressively less used in investor decisions has limited value.

A Different Technology

Automated trading accounts for at least 75 percent of corporate stock trades (Prakash 2016; Bute 2016) and is often affected by changes in stock price and volume over very short time intervals and not by any intrinsic economic performance data (Demos 2012; Wigglesworth 2016). Variables such as inventory (for just-in-time management), overnight cash balances

The authors are thankful for the helpful comments and advice of Dorothy McQuilken, Chris Halterman, Andrea Rozario, and Jamie Freiman during the formulation of this editorial.

Published Online: July 2017

[1] ISA 701 (https://www.ifac.org/publications-resources/international-standard-auditing-isa-701-new-communicating-key-audit-matters-i) requires the disclosure of key audit matters that open the opportunity of a less binary opinion. Key audit matters pertain to matters the auditor deems to be of the most significance (e.g., complex revenue transactions, tax-related matters, goodwill impairment) in the audit of financial statements of the current period. The auditor is required to communicate on the audit report the matters that require significant judgment, the types of risks those matters present, how the auditor plans to respond to those risks, and the results/findings of the procedures applied in response to the risks.

(for application and sourcing of overnight loans), and accounts receivables and payables (for discounting), together with many other items, are necessary and available in modern systems either in close to real-time systems, or through networking with closely connected systems. However, data latency in such systems results in the poor usage of corporate resources (*The Economist* 2017; Alles, Brennan, Kogan, and Vasarhelyi 2006; Alles, Kogan, and Vasarhelyi 2008) and inadequate competitive positioning. Furthermore, GAAP has not evolved to adopt rapidly changing corporate information processing, the emergence of Big Data sources (Vasarhelyi, Kogan, and Tuttle 2015; Krahel and Titera 2015), or advanced analytic methodologies. This modern world of close-to-event measurement is going to be progressively linked to predictive analytics as the primary need of investors' shifts from assessing the performance of stocks in the past, to focusing on future performance estimates. The toolset of these predictions has substantially improved in recent years. Although current corporate statements may include predictions, they are essentially backward-looking documents. A wide range of predictive methodologies are now available and have been practically implemented (Siegel 2013; Koch 2015). Hence, it is natural that these methodologies evolve into the corporate measurement arena.

Different Needs of Stakeholders

The aforementioned automated trading is a blatant example of the gap that has emerged between user needs and what the business measurement and assurance community are providing. In many areas of business measurement, this gap has evolved and also provides stimulus for large amounts of supplemental, and often anachronistic, information requirements. The analyst community has for a long time used additional information in its work, but it also suffers from having to apply old information to a real-time set of processes, where day trading or automatic trading focuses on volume and up and down ticks on price instead of substantive value information. A progressively more real-time environment can benefit from assurance in many dimensions and improve the entire business measurement and operations environment. Consequently, the traditional audit frame should be modified to allow a set of assurance services in a modern age and include (1) continuous (internal and external) audit, (2) continuous control monitoring, and (3) continuous cybersecurity assurance.

In sum, the traditional audit model should be revisited for the development of new assurance services, especially with regard to cybersecurity and continuous assurance. In the next section, we discuss three basic elements of the traditional audit model that need to be reconsidered.

CHANGING THE NATURE OF GENERALLY ACCEPTED AUDITING STANDARDS (GAAS) TO NEW GAAS (NGAAS)

Point in Time Report

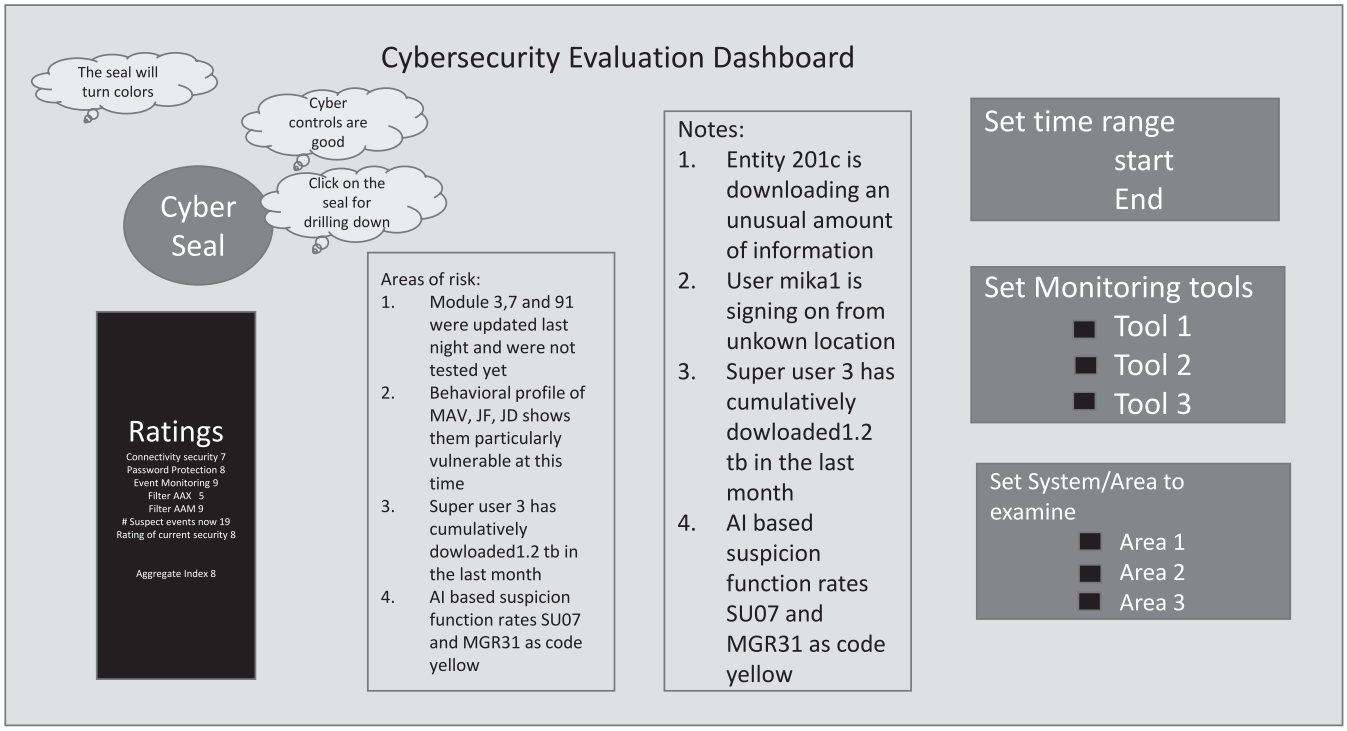
As corporate systems are live, continuously changing, and under continuous threat, it is crucial to have real-time internal reporting that fairly represents the current status of the systems to multiple stakeholders.[2] For instance, cybersecurity is not a point in time representable phenomenon, but rather, as noted by the AICPA (2017a), it is an aggregate of parameters such as governance, control procedures, risk status, and data status. At any point in time, all systems, especially large systems, have some form of security breach (Mitra and Ransbotham 2015) from the trivial, where an employee allows someone else to use his or her passwords, to massive data breaches, such as Yahoo Inc.'s leak of over a billion records over a two-year period before detection. An opinion about (or assurance of) cybersecurity is not likely directly applicable to a given point in time, but should be related to a period in time and be based on multivariate estimates of different cybersecurity factors such as organizational characteristics and the nature of the operations and information at risk. During the period of coverage, real-time tools and measurements need to remain in operation, to be published for access by the public or stakeholders, and to be available for the application of external analytics. Due to the nature of problems, controls, and defenses, some measurements may be highly private and dynamic in nature.

The Zero/One Nature of an Opinion

The current assurance model requires an organization's audit committee to hire external auditors, as well as to make decisions about fees, retention, and sometimes inputs into the scope of work. Furthermore, there are serious limitations on the usage of client peer data during traditional audit engagements. The current zero/one audit opinion of whether the financial statements of an entity are presented fairly in all material respects and in accordance with GAAP is unlikely applicable to new assurance services such as cybersecurity and continuous assurance, and thus becomes an obstacle for assurers providing such

[2] Stakeholders include a large population of directly related parties such as investors, suppliers, customers, and banks, as well as indirectly related parties such as internal and external auditors, regulators, and localities.

FIGURE 1
Cybersecurity Dashboard and Seal Concept



services. For instance, an assurance engagement on cybersecurity likely focuses on the effectiveness of an organization's cybersecurity risk management. A better fit for the cybersecurity assurance model would be:

- Online real-time monitoring of cybersecurity
- Continuous rating, by automatic tools, of system/company security status
- Selective disclosure of security tools, settings, and security events[3] (e.g., security breaches)
- Shared and standardized databases on identified security events[4]

Furthermore, additional information is needed about the other components (control environment, risk assessment, risk activities) for effective decision making.

As discussed above, a "clean" audit opinion is not really applicable for either cybersecurity or continuous assurance, as faults of a qualitative nature or nonmeasurable magnitude may arise at any time. A dashboard (Figure 1) of cybersecurity risk or of data and control risk (e.g., McKenna, Staheli, Fulcher, and Meyer 2016) may provide better value to stockholders while reducing the potential of spurious litigation of little value to the stakeholders and of potential large risk to the assurors. This dashboard could be used as a proxy for the auditor's opinion if set to point in time, zero/one, and monetary materiality thresholds. Its setting would allow substantive evaluation through drill downs, time ranges, monitoring tool outputs, and other factors.

The Concept of a Fair Representation Threshold (Materiality)

Generally Accepted Auditing Standards (GAAS) prescribe a rather vague concept of materiality, which is often interpreted as a dollar amount related to steady state net income potential. However, many cybersecurity exposures in areas such as sustainability, supply chain, brand, and risk perception may not be measured in monetary terms and consequently do not fit well

[3] Unlike financial reporting, the disclosure of security events and setups may have detrimental effects on organizations' security and may present opportunities to hackers. Common guidance on what needs to and should be disclosed may be necessary.

[4] Companies are very hesitant to share exposures and cyber events. This hesitation is realistic and mechanisms such as anonymization, regulations, and standardization must be created for enablement of cyber information sharing. This same information may also be a source of danger to companies.

into this conceptualization. New forms of allowable error in measurement must be developed for incorporation into new GAAS.

In short, for the development of new assurance services, the traditional audit model should reconsider three basic elements: the point in time report, the zero/one nature of an opinion, and the concept of a fair representation threshold. In the next section, we discuss the influence of these elements on cybersecurity and continuous assurance services.

CONTINUOUS ASSURANCE UNDER NEW GAAS

Vasarhelyi and Halper (1991) described an application developed by AT&T Bell Laboratories that monitored and provided internal audit assurance to, what was at that time, AT&Ts world's largest customer billing system. This application extracted data from a variety of customer reports, applied a wide variety of monitoring algorithms, and compared this with models (i.e., standards) to create alerts for anomalies within the system. This system was somewhat analogous to the one proposed by Groomer and Murthy (1989), who argued for embedded audit modules, but its data collection and processes were not embedded. This work eventually established the basis for CICA and AICPA's (1999) publication on *Continuous Auditing: Research Report*. This monograph defines a continuous audit as "a methodology that enables independent auditors to provide written assurance on a subject matter, for which an entity's management is responsible, using a series of auditors' reports issued virtually simultaneously with, or a short period of time after, the occurrence of events underlying the subject matter" (CICA and AICPA 1999).

Continuous Data Assurance (CDA)

While parts of this definition, such as its emphasis on "written assurance," have been made obsolete by the progress of technology, the definition has helped jumpstart a thriving research field as well as industry practices involving continuous assurance. A comprehensive literature review on continuous assurance can be found in Brown, Wong, and Baldwin (2007) and Chiu, Liu, and Vasarhelyi (2014). With the advent of Continuous Controls Monitoring (CCM) and Continuous Risk Monitoring and Assessment (CRMA), also to be discussed in this section, the data monitoring/assurance process has been renamed Continuous Data Assurance (CDA). Technological changes and evolution not only permit close to real-time monitoring of data, but also support of the concept of "Audit by Exception" (ABE). Vasarhelyi and Halper (1991) define the Continuous Process Audit System (CPAS) approach as "a philosophy of auditing that aims to monitor key corporate processes on a continuous basis, in order to achieve audit by exception," and argue that "the methodology will change the nature of evidence, timing, procedures, and effort involved in audit work."

Byrnes, Ames, and Vasarhelyi (2015) examined the adoption of continuous audit and concluded that by and large, CPA firms were not using Continuous Assurance (CA). On the other hand, Vasarhelyi, Alles, Kuenkaikaew, and Littley (2012) examined the internal audit practices of nine firms and found deeper interest and incipient usage of CA. Bumgarner and Vasarhelyi (2015) proposed a new view of CA, yet have not engaged in the important task of separating CA from the traditional audit model under the three elements necessary for new GAAS. These three elements are:

1. *Continuous, not point in time, opinions* that could be achieved by system monitors that examine the audit ecosystem (Kozlowski 2016) constantly and rate the level of exceptions being found in ABE.
2. *A system of rating accuracy*[5] not a zero/one opinion (fair or not fair representation with "subject to" restrictions and qualifications).
3. *A hybrid method of measurement of fair representation* that is not purely quantitative.

A fourth element may be added:

4. *Use of a dashboard and/or a seal* (Figure 1) to display the opinion as opposed to a traditional paper-based opinion.

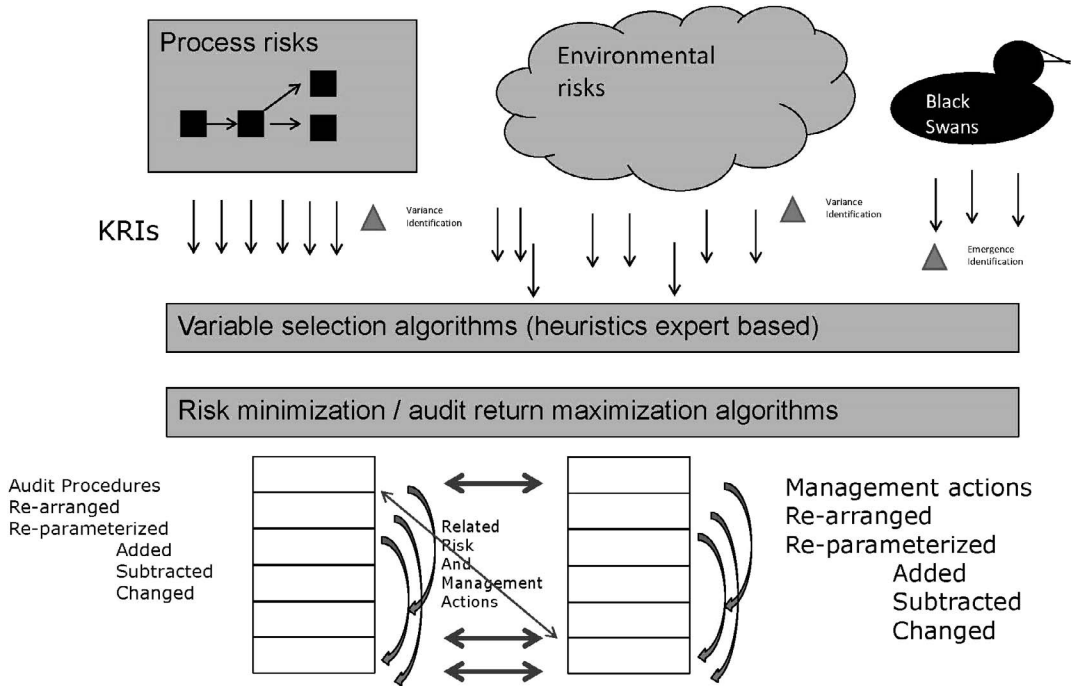
These three variations from GAAS, as well as a dashboard and/or seal, would open new horizons in assurance and allow for a real CA. Conceivably, CDA would entail the above-mentioned configurable audit seal[6] reflecting the number and type of exceptions at a particular variable point in time. Stakeholders could monitor these seals with software agents[7] and be warned about important arising exceptions. If the requirements of GAAS need to be satisfied, then the variable time frame would be set to one year, and the concept of fair representation could be parameterized monetarily at, say, 5 percent of long-term net income.

[5] The recent requirement of disclosure of key audit matters by the International Auditing and Assurance Standards Board (IAASB) opens a possibility of a more detailed rating of accuracy. Its implementation, to be observed, will determine whether this is the case.

[6] Patent proposal, Real Seal, February 11, 1999, AT&T Bell Laboratories.

[7] Software agent refers to a computer program that can perform complex tasks on behalf of a user or other program.

FIGURE 2
Schemata of CRMA Progress
(Vasarhelyi et al. 2012)



Continuous Control Monitoring (CCM)

Alles et al. (2006) described an application of control monitoring performed by Siemens AG's internal audit that extracted control configurations of an SAP facility and compared them with a baseline. The occurrence of a significant variance (i.e., larger than the allowable variance) was called an alert or alarm. This application was named as Continuous Control Monitoring (CCM) and was incorporated as the second element of the continuous audit, as displayed in Figure 3.

Continuous Risk Monitoring and Assessment (CRMA)

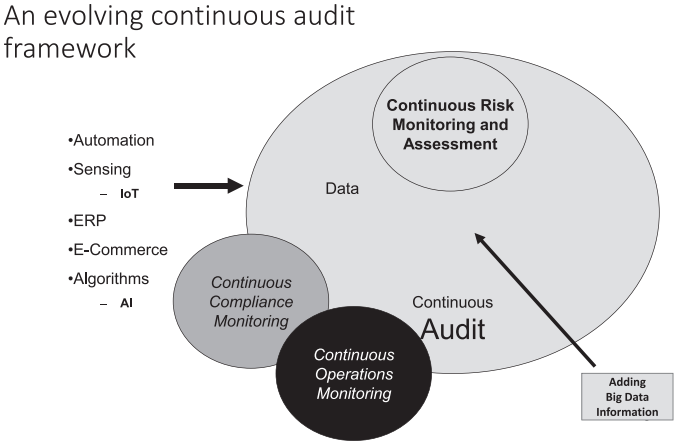
Finally, recent pressure from the Public Company Accounting Oversight Board (PCAOB) for firms to perform a "risk-based audit" has caused the emergence of the third element of the traditional view of continuous audit—Continuous Risk Monitoring and Assessment (CRMA). In CRMA (Figure 2), Key Risk Indicators (KRIs) (Scandizzo 2005) are identified within the company's operations and environment. The identified KRIs are called black swans, which are noteworthy potential risks with a very low probability of occurrence (Taleb 2010). KRIs are monitored, and optimization procedures are used to balance observed and contravening risks. Once risks are balanced, an audit program is developed. When significant changes are observed in one of several KRIs, an adjusted audit program may be generated that also considers what steps were already performed in the audit. Additionally, if observed risks are important for management action, then internal auditors discuss with executives to discover what steps need to be taken and plan audit changes accordingly. This is described in Figure 2.

These three elements together represent continuous auditing. However, other related processes also overlap, complement, or confuse this conceptualization. Vasarhelyi et al. (2012) surveyed nine leading internal audit departments and concluded that there are many "audit-like" departments or functions that act typically independently and with varied levels of technological utilization. Figure 3 points out that in modern organizations, both compliance[8] efforts and operations monitoring efforts could be considered as complementary to the continuous audit.

Furthermore, in addition to internal data capture and processing methods, organizations rapidly take advantage of Big Data sources to serve many functions such as market targeting, serving ads, and driving investments. The assurance world, despite a

[8] Cloud Conformity (see, https://www.cloudconformity.com/) offers 200 indices of compliance in a compliance monitoring product.

FIGURE 3
Related Elements of Continuous Audit



large amount of interest, is lagging substantially in the usage of these applications (Vasarhelyi et al. 2015). In order to further stress the usage of GAAS, several points must be mentioned to this end. In general, Big Data sources are less precise as sources of evidence and have not been formally considered in audit standards. The evaluation of the provenance (Appelbaum 2016; Appelbaum, Kogan, and Vasarhelyi 2017), the collection (availability) of the data, the need to sift through the data (Anderson 2008) before collection and retention, and a lack of theory behind empirically based models (Chiu et al. 2014) are related issues that make audit standards (methods) open for reconsideration. Exploratory data analysis (Tukey 1977) should be performed first, and then used to serve as the basis for assertion selection. Standards do not yet deal with the nature of Big Data, the methods used to apply Big Data sources to the audit, or their value as evidence.

Figure 3 points out that the three complementary elements of continuous assurance in a modern organization, when complemented by both compliance efforts and operations monitoring efforts, will enable progressively larger uses of big exogenous information.

Continuous Compliance and Operations Monitoring

As organizations currently operate in a world of intense regulation, their exposure to compliance issues is very large. The nature of operations still tends to be very manual, but progressively vendors and companies are deriving analytic methods for different forms of compliance verification. Again, compliance, a process that could be continuous in nature if automated, does not fit very well into a point in time report, the zero/one nature of an opinion, or a monetary-based evaluation (materiality). The methods used for compliance monitoring overlap with day-to-day operations monitoring, and many of the systems that can perform these functions are also the basic foundations for a continuous audit. Although some companies have very separate continuous audit systems, without the baseline of operation monitoring, a continuous audit cannot be performed. Table 1 relates the elements of Figure 3 to system users. It also raises the question of the role of intelligent systems (Tschakert, Kokina, Kozlowski, and Vasarhelyi 2016) in these functions.

CYBERSECURITY ASSURANCE IN NEW GAAS

In this section, we discuss a very different issue, also currently of interest to the audit community, which is assurance needs that do not fit very well with the traditional audit model.

Cybersecurity

Cybersecurity is an umbrella concept that encompasses information security and information assurance. It is often used interchangeably with the term information security. Information security is related to the preservation of the confidentiality, integrity, and availability of information, and was defined by Whitman and Mattord (2011) as "the protection of information and its critical characteristics (confidentiality, integrity, and availability), including the systems and hardware that use, store, and transmit that information, through the application of policy, training and awareness programs, and technology." On the other hand, information assurance refers to the technical and managerial measures involved in protecting information systems and is defined as "the practice of assuring information and managing risks related to the use, processing, storage, and

TABLE 1

Users, Purpose, and Approach of the Elements of Continuous Assurance

	Data Assurance	Controls	Compliance	Risk Monitoring and Assessment	Operations (Monitoring)
Who Uses					
Management	X	X	X	X	X
Audit (Internal or External)	X	X	X		
Investors	X				
Regulators	X	X	X		
Purpose					
Diagnostic		X	X	X	X
Predictive				X	X
Historic	X	X	X	X	X
Primarily Performed by					
Automation	X	X	X	X	X
Manual		X		X	X
Intelligent System	X	X	X	X	X

Adapted from Bumgarner and Vasarhelyi (2015).

transmission of information or data and the systems and processes used for those purposes" (Wikipedia 2017). In accordance with the above definitions, the AICPA defines cybersecurity as "the process of applying security measures to ensure confidentiality, integrity, and availability of data" (AICPA 2017b). Thus, cybersecurity is a collection of technologies, processes, and practices that safeguard and assure the protection of an organization's assets such as information and systems.

Technology Giveth, Technology Taketh

Technology plays a crucial role in any organization. Public and private companies, banks, and governments benefit by adopting new technology to fulfill their daily operations needs and to accomplish their business objectives. Technologies, such as personal computers, the internet, and cloud computing, have provided tremendous prosperity to organizations over the last decade. Just as new technology brings greater opportunities, such as automated processes, better access and connectivity, and improved sharing of information, it also brings greater challenges. In particular, the opportunities that new technology provides often lead to security threats (i.e., become a focal point for cyberattacks). Hence, for many of the new technologies developed, other new technologies are necessitated for their defense. Many current cybersecurity solutions available in the market either provide single-point defense mechanisms for known types of cyberattacks, or rely on experienced security experts who can build complex defense mechanisms to prevent, detect, and remediate cyberattacks. As organizations incorporate new technologies into their systems that enhance cybersecurity, hackers or intruders continue to evolve and develop new attack strategies or mechanisms designed to penetrate these systems.

Should Auditors Be Involved in Cybersecurity?

The first issue is whether auditors should be involved in cybersecurity. This issue entails a series of considerations that are difficult to establish. First, cybersecurity can clearly influence the economic health of an organization. This can even apply to the extreme degree of affecting a company's going concern status. Ponemon Institute (2013, 2015) estimated the average cost of cyberattacks to be $11.6 million per organization for 2013, which was 26 percent larger than in 2012. This per organization cost for 2015 was $15 million. In addition, according to the BI Intelligence in Business Insider (2016), organizations are expected to spend $655 billion on cybersecurity initiatives between 2015 and 2020. Second, auditor competence in this highly technical area raises questions. Clearly, current auditors are neither trained nor tested in cybersecurity issues.[9] They do, however, have training in other subject matters that may overlap with cybersecurity, such as a valuation where the auditor relies on specialists to support key assertions. While some firms do provide IT audit specialization skills to their employees, the greater scope of accountant training precludes these skills, and such a specialty is not acknowledged or required in any portion of the current CPA certification. Third, if not auditors, then who should take the role of integrating financial and cyber risk

[9] Many CPAs are IT audit specialist and may hold additional certifications such as Certified Information Systems Auditor (CISA) or Certified Information Systems Security Professional (CISSP). However, the number with the necessary skills is not sufficient.

information into some form of assurance that can be provided to shareholders? Finally, and most important, can the risk assessment portion of future audits be performed without the consideration of cybersecurity? The answer is most likely no, but substantive research is needed on how to integrate the generally qualitative issues of risk of cyber exposure into the traditional audit model.

Is Cybersecurity a Longer-Range Issue and Problem?

As we addressed, along with new technology development, cybersecurity threats are rapidly changing and evolving, fast in pace, and are requiring great attention. It is important, although difficult, for organizations to stay current with cybersecurity issues. In the case of many cybersecurity attacks, hackers or intruders often lock on a specific target and prepare long-range plans to achieve their goals. Therefore, anticipating threats and assessing security vulnerabilities in information systems is a long-term issue. There is no short-term solution. This process requires not only a comprehensive approach on the part of organizations, but a continuous effort as well. However, many organizations often consider cybersecurity as an expense with little return. This misconception results in inadequate management support of such programs, which in turn leads to poorly designed security systems and policies. Therefore, it is critical for organizations to take a long-term approach regarding their cybersecurity initiatives in order to protect the critical systems and assets that are vital to them. The key is to plan a long-term cybersecurity solution that impacts all levels of organizations and systems, and that assures the protection of organization's systems and assets.

Cybersecurity and Continuous Audit (Assurance)

Both cybersecurity and continuous assurance do not fit well into the GAAS. Both need to be real time, as well as relate to a time period. Both have nuances that cannot be expressed in "fairly represents" reporting models, and both are not amenable to a monetary materiality threshold related directly to value. Table 2 displays the issues and potential solutions.

FORCE-FEEDING THE TRADITIONAL AUDIT MODEL

The cybersecurity guide being issued by the AICPA presents a set of problems where the current reporting and attestation standards do not fit properly. Designed to perform under Attestation Standards AT-C Sections 105 (*Concepts Common to All Attestation Engagements,* available at: https://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AT-C-00105.pdf) and 205 (*Examination Engagements,* available at: https://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AT-C-00205.pdf), the new cybersecurity guide places sets of attestation criteria into two categories: description criteria and control criteria. The former criteria are designed to prepare and evaluate the presentation and description of an organization's cybersecurity risk management, whereas the later criteria are devised for determining the effectiveness of controls to accomplish the organization's cybersecurity objectives. This more traditional approach to criteria definition neglects to incorporate the ever-changing nature of cybersecurity threats. It does not, for example, incorporate an analysis of the potential effects that a failure in a cybersecurity system may have on a given business.[10] As business adoption of technology varies, these impacts must be determined on an engagement-to-engagement basis. Furthermore, a group of analytic technologies and processes have emerged and serve to improve attestation or audit quality. However, such analytic technologies and processes do not conform well to the traditional audit standards. The entire audit process (as characterized in Table 3) may be progressively changed as pointed out in the table's highlights. There, an overall, semi-autonomous, automation rich assurance process will emerge with several types of objectives and potential products. The profession may greatly benefit from this product emergence, but if it does not create an agile mechanism of change, then it may lose this business opportunity to other parties.

Auditor Qualification

Current education and professional qualifications tend to be all in one. The accounting graduate is an audit professional, but he or she is poorly qualified in the statistical, IT, and modeling skills needed in the modern audit profession. Typically, larger firms have separate advisory groups that are used in the case of specialist needs during an engagement. However, even understanding the need to seek the aid from such a group requires a certain level of education that is not prevalent. (PCAOB 2002). Papers such as Tschakert et al. (2016) and Appelbaum, Showalter, Sun, and Vasarhelyi (2015) have discussed the issues facing audit education.

[10] This may however, be remedied by key audit matters disclosure, as discussed earlier under the international audit standards.

TABLE 2

Potential Features on NGAAS Standards Based on CA and Cybersecurity Issues

	Continuous Assurance	Cybersecurity	Potential Solution
Point in Time	• Time frame is a range and close to the event measurement.	• Time frame is a range and close to the event measurement. Most likely, there are always some degrees of breaks that cannot be detected/identified.	• Real seal and adjustable dashboard.
Zero/One Opinion with "Subject to"	• Better measurement with multiple parameters. • Must be careful not to always give top of the range evaluations.	• Better measurement with multiple parameters. • Must be careful not to always give top of the range evaluations. • Maturity model also has been proposed as a rating scheme.	• Multivariate opinion ratings on pre-set industry criteria disclosed with average line-of-business rating ranges.
Numerical Materiality	• It is difficult for a continuous monitoring process to establish numerical materiality per transaction. • Typically, each exception type has its alarm threshold.	• The danger of a cyber-break depends on a multitude of parameters that are most likely not numerical.	• Questionnaires and qualitative determination of danger and impact of each type of known intrusion and methods of detecting unknown intrusions.
Verbal Expression of the Opinion	• "Fairly represents" does not fit well. • "Meets criteria" as in the guide is better.	• "Fairly represents" does not fit well.	• Different types of sentences representing some of the characteristics of the multivariate opinion ratings.

Unintended Consequences

The disclosure of details on cybersecurity or its rating may bring increased exposure to both well-rated companies and poorly rated companies. For hackers, well-rated companies can be considered as challenges. Alternatively, hackers may also concentrate on those firms reported as having poor security.

A continuous assurance seal requires active monitoring of exceptions and possibly a violation of the anti-consulting provisions of the Sarbanes-Oxley Act.

The inclusion of cybersecurity into the assurance umbrella may bring increased litigation toward the audit profession if some of these concerns of the extant audit model are not resolved. The fact that auditors are not allowed to also consult for their clients has brought about some de-technologization of the profession, where auditors do not do any more work together with their technical consulting counterparts. It is difficult to predict what the organization of the large firms will look like and what the auditor's skill mix will be if several of these products are adopted and if the smaller firms find ways to compete.

Other Forms of Attestation

The AICPA has attempted other forms of attestation such as WebTrust and Systrust, but these products did not manage to gain any traction, probably because they were visionary products before the profession was ready to change. Subsequently, the AICPA generated the principles and criteria of trust services and posteriorly created Service Organization Control (SOC) 1 and SOC 2, which have been much more successful.

CONCLUSIONS: THE ASSURANCE ECOSYSTEM

This paper discusses the challenges that the traditional audit model poses upon modern technology-based systems, as well as the need for technological assurance. It examines continuous audit and cybersecurity as two of the potentially many settings in which a new set of GAAS could be applied. Although there are many features of GAAS that could, and eventually will be, modernized, this paper focuses on point in time reporting, the zero/one option of opinions, and the concept of a fair representation threshold (i.e., materiality). Other features are also discussed.

The distance between management (and assurers) and their data (both internal and external) is growing larger and larger every day. Automation is now progressively taking over many of the accounting functions (Monga 2015). Robots and intelligent algorithms are going to progressively replace layers of repetitive work, and formalize many parts of the accounting

TABLE 3

Audit Phases and Analytic Methods

Audit Phase	Applicable Analytic Methods	Observations	Highlights
Client Examination	• News media monitoring • Social media monitoring	• A large set of sources allows for environmental scanning of events with directors, their reputation, the behavior of competitors, and events in the industry.	
Audit Planning	• *Ex ante* risk assessment *a la* CRMA • Ratio analysis	• Peer industry group evaluation for performance.	• CRMA processes will complement the audit planning process by taking a dynamic evaluation of KRIs. • Values from the cybersecurity assessment and monitoring will be considered.
Audit Risk Assessment	• CRMA	• The "material" change in the risk situation requires changes in continuous monitoring, management action, and in continuous audit parameters.	• Risk assessments will drive the levels of monitoring and include live evaluation "apps" and cybersecurity monitors based on KRIs and data from key monitoring.
Internal Control Evaluation	• Process mining • Analytical modeling	• Reliance on the "best of class" nature of designed ERP systems, but hampered by the fact that most large organizations' data are from a mix of ERP based and other type sources.	
Compliance Testing	• Process mining • CCM	• Concern about user configurable controls requires monitoring these settings through a CCM methodology.	• Monitoring of compliance on aggregate indicators will affect internal control evaluation. In the controls area, audit and cyber indicators will overlap and cooperate.
Substantive Testing	• Cluster analysis • Database-to-database confirmations • Continuity equations	• The emergence of very large number of transactions, the ability to store them online, the reliance on electronic documents and records, and the usage of XML derivative languages to exchange data from upstream and to downstream systems changed drastically the items to be tested and requires new audit tests that are not yet in the vernacular.	• Substantive tests will be constantly run by software agents, in particular over data coming into the system. • Exogenous data sources such as social media, weather, regional micro-economic, and IoT will confirm and complement cyber and assurance data. Those two data will be somewhat interchangeable.
Opinion Formulation	• Formal expert systems for the evaluation of new forms of audit evidence • Systems for estimating potential for audit failure based on internal evidence and exogenous variables	• With the multitude and volume of data forms, and the lack of direct observability of data, audit systems will have to be substantially automated with a symbiotic process of opinion formulation, partially relying on machine observation and opinion formulation.	• As seals will have to be formed, the level of "suspicion" of the system will have to be not intuitively judgmental but formally determined, as it will depend on machine formulation. An overlay of human judgment most likely will, for a long time, be necessary. • Different graduated opinions may exist with different audit products such as monitoring operations product, financial assurance product, control monitoring product, and cybersecurity product.

Modified Schema of Cushing and Loebbecke (1986).

and audit profession (Issa, Sun, and Vasarhelyi 2016; McAfee and Brynjolfsson 2016; Chui, Manyika, and Miremadi 2015). The standards and methods proposed here would be part of a larger ecosystem of business measurement and assurance with a large set of components being automated, and the extreme interpretation, decision making, and exception treatment resting in the hands of humans.

—Won Gyun No
—Miklos A.Vasarhelyi
Rutgers, The State University of New Jersey, Newark

REFERENCES

Alles, M. G., A. Kogan, and M. A. Vasarhelyi. 2008. Putting continuous auditing theory into practice: Lessons from two pilot implementations. *Journal of Information Systems* 22 (2): 195–214. doi:10.2308/jis.2008.22.2.195

Alles, M., G. Brennan, A. Kogan, and M. A. Vasarhelyi. 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. doi:10.1016/j.accinf.2005.10.004

American Institute of CPAs (AICPA). 2016. *AICPA Proposes Criteria for Cybersecurity Risk Management*. Available at: http://www.aicpa.org/Press/PressReleases/2016/Pages/AICPA-Proposes-Criteria-for-Cybersecurity-Risk-Management.aspx

American Institute of Certified Public Accountants (AICPA). 2017a. *Proposed Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program*. Available at: http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/DownloadableDocuments/ExposureDrafts/ASEC_ED_Criteria_Cyber_Engagement.pdf

American Institute of Certified Public Accountants (AICPA). 2017b. *Security and Privacy*. Available at: https://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/Pages/default.aspx

Anderson, C. 2008. *The End of Theory: The Data Deluge Makes the Scientific Method Obsolete*. Available at: https://www.wired.com/2008/06/pb-theory/

Appelbaum, D. 2016. Securing Big Data provenance for auditors: The Big Data provenance black box as reliable evidence. *Journal of Emerging Technologies in Accounting* 13 (1): 17–36. doi:10.2308/jeta-51473

Appelbaum, D., A. Kogan, and M. A. Vasarhelyi. 2017. Big Data and analytics in the modern audit engagement: Research needs. *Auditing: A Journal of Practice & Theory* ajpt-51684. doi:10.2308/ajpt-51684

Appelbaum, D., D. S. Showalter, T. Sun, and M. A. Vasarhelyi. 2015. Analytics knowledge required of a modern CPA in this real-time economy: A normative position. *Proceeding of the Accounting Information Systems Educator Conference,* Colorado Springs, CO.

Ball, R., and P. Brown. 1968. An empirical evaluation of accounting income numbers. *Journal of Accounting Research* 6 (2): 159–178. doi:10.2307/2490232

Brown, C. E., J. A. Wong, and A. A. Baldwin. 2007. A review and analysis of the existing research streams in continuous auditing. *Journal of Emerging Technologies in Accounting* 4 (1): 1–28. doi:10.2308/jeta.2007.4.1.1

Bumgarner, N., and M. A. Vasarhelyi. 2015. Auditing—A new view. In *Audit Analytics and Continuous Audit: Looking Toward the Future*. Available at: https://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/DownloadableDocuments/AuditAnalytics_LookingTowardFuture.pdf

Business Insider. 2016. *This One Chart Explains Why Cybersecurity Is So Important*. Available at: http://www.businessinsider.com/cybersecurity-report-threats-and-opportunities-2016-3

Bute, J. B. 2016. *The Self-Fulfilling Prophecy of Automated Stock Trading*. Available at: https://www.washingtonpost.com/opinions/the-self-fulfilling-prophecy-of-automated-stock-trading/2016/01/26/c983b91c-c37d-11e5-b933-31c93021392a_story.html?utm_term=.605efcbea6a5

Byrnes, P. E., B. Ames, and M. A. Vasarhelyi. 2015. The current state of continuous auditing and continuous monitoring. In *Audit Analytics and Continuous Audit: Looking Toward the Future*. Available at: https://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/DownloadableDocuments/AuditAnalytics_LookingTowardFuture.pdf

Canadian Institute of Chartered Accountants, and American Institute of Certified Public Accountants (CICA and AICPA). 1999. *Continuous Auditing: Research Report*. Toronto, Canada: CICA and AICPA.

Chiu, V., Q. Liu, and M. A. Vasarhelyi. 2014. The development and intellectual structure of continuous auditing research. *Journal of Accounting Literature* 33 (1/2): 37–57. doi:10.1016/j.acclit.2014.08.001

Chui, M., J. Manyika, and M. Miremadi. 2015. Four fundamentals of workplace automation. *McKinsey Quarterly* (November): 1–9.

Cushing, B. E., and J. K. Loebbecke. 1986. *Comparison of Audit Methodologies of Large Accounting Firms*. Sarasota, FL: American Accounting Association.

Demos, T. 2012. *"Real" Investors Eclipsed by Fast Trading*. Available at: https://www.ft.com/content/da5d033c-8e1c-11e1-bf8f-00144feab49a

Eccles, R. G., and M. P. Krzus. 2010. *One Report: Integrated Reporting for a Sustainable Strategy*. Hoboken, NJ: John Wiley & Sons.

Economist, The. 2001. *Computing Power on Tap*. Available at: http://www.economist.com/node/662301.

Groomer, S. M., and U. S. Murthy. 1989. Continuous auditing of database applications: An embedded audit module approach. *Journal of Information Systems* 3 (2): 53.

Issa, H., T. Sun, and M. A. Vasarhelyi. 2016. Research ideas for artificial intelligence in auditing: The formalization of audit and workforce supplementation. *Journal of Emerging Technologies in Accounting* 13 (2): 1–20. doi:10.2308/jeta-10511

Koch, R. 2015. From business intelligence to predictive analytics. *Strategic Finance* 96 (7): 56.

Kozlowski, S. 2016. *A Vision of an ENHanced ANalytic Constituent Environment: ENHANCE*. Ph.D. dissertation, Rutgers, The State University of New Jersey Graduate School.

Krahel, J. P., and W. R. Titera. 2015. Consequences of Big Data and formalization on accounting and auditing standards. *Accounting Horizons* 29 (2): 409–422. doi:10.2308/acch-51065

Lev, B. 1989. On the usefulness of earnings and earnings research: Lessons and directions from two decades of empirical research. *Journal of Accounting Research* 27: 153–192. doi:10.2307/2491070

McAfee, A., and E. Brynjolfsson. 2016. Human work in the robotic future. *Foreign Affairs* 95 (4): 139–150.

McKenna, S., D. Staheli, C. Fulcher, and M. Meyer. 2016. *BubbleNet: A Cyber Security Dashboard for Visualizing Patterns*. Available at: http://onlinelibrary.wiley.com/doi/10.1111/cgf.12904/full

Mitra, S., and S. Ransbotham. 2015. Information disclosure and the diffusion of information security attacks. *Information Systems Research* 26 (3): 565–584. doi:10.1287/isre.2015.0587

Monga, V. 2015. *The New Bookkeeper Is a Robot*. Available at: https://www.wsj.com/articles/the-new-bookkeeper-is-a-robot-1430776272

Pacioli, L. 1494. *Summa de Arithmetica, Geometria, Proportioni et Proportionalita*. Venice, Italy: Paganino de Paganini.

Ponemon Institute. 2013. *2013 Cost of Cyber Crime Study: United States*. Available at: https://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf

Ponemon Institute. 2015. *2015 Cost of Cyber Crime Study: United States*. Available at: http://www.ponemon.org/blog/2015-cost-of-cyber-crime-united-states

Prakash, A. 2016. *Rocky Markets Test the Rise of Amateur "Algo" Traders*. Available at: http://www.reuters.com/article/us-europe-stocks-algos-insight-idUSKCN0V61T6

Public Company Accounting Oversight Board (PCAOB). 2002. *AS 2305: Substantive Analytical Procedures*. Available at: https://pcaobus.org/Standards/Auditing/Pages/AS2305.aspx

Sangster, A. 2016. The genesis of double entry bookkeeping. *The Accounting Review* 91 (1): 299–315. doi:10.2308/accr-51115

Scandizzo, S. 2005. Risk mapping and key risk indicators in operational risk management. *Economic Notes* 34 (2): 231–256. doi:10.1111/j.0391-5026.2005.00150.x

Schaltegger, S., M. Bennett, and R. Burritt, eds. 2006. *Sustainability Accounting and Reporting*. Volume 21. New York, NY: Springer Science & Business Media. doi:10.1007/978-1-4020-4974-3

Siegel, E. 2013. *Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die*. New York, NY: John Wiley & Sons.

Taleb, N. N. 2010. *The Black Swan: The Impact of the Highly Improbable*. 2nd edition, Volume 2. New York, NY: Random House.

Tschakert, N., J. Kokina, S. Kozlowski, and M. Vasarhelyi. 2016. The next frontier in data analytics. *Journal of Accountancy* 222 (2): 58–63.

Tukey, J. W. 1977. *Exploratory Data Analysis*. Boston, MA: Addison-Wesley Pub. Co.

Vasarhelyi, M. A., and F. B. Halper. 1991. The continuous audit of online systems. *Auditing: A Journal of Practice & Theory* 10 (1).

Vasarhelyi, M. A., A. Kogan, and B. M. Tuttle. 2015. Big Data in accounting: An overview. *Accounting Horizons* 29 (2): 381–396. doi:10.2308/acch-51071

Vasarhelyi, M. A., M. Alles, S. Kuenkaikaew, and J. Littley. 2012. The acceptance and adoption of continuous auditing by internal auditors: A micro analysis. *International Journal of Accounting Information Systems* 13 (3): 267–281. doi:10.1016/j.accinf.2012.06.011

Whitman, M. E., and H. J. Mattord. 2011. *Principles of Information Security*. 4th edition. Mason, OH: Cengage Learning.

Wigglesworth, R. 2016. *Investment: Rise of the DIY Algo Traders*. Available at: https://www.ft.com/content/0a706330-5f28-11e6-ae3f-77baadeb1c93

Wikipedia. 2016. Information assurance. Available at: https://en.wikipedia.org/wiki/Information_assurance