# The Coming Age of Continuous Assurance

Miklos A. Vasarhelyi[1]

A condensed version of the 71st CPA Australia/University of Melbourne Annual Research Lecture presented on 11 October 2010. A recorded version of the lecture can be found at ... [Geoff to obtain details]

## *Introduction*

In recent decades, businesses worldwide have been transformed by powerful information technologies to operate in what has been labelled the 'now economy', characterised by 24-hour globalised operations, customer interactions and management decisions. These electronic transformations have affected the entire business cycle by incorporating a multiplicity of technologies into organisational processes. Financial processes have also evolved substantially, supported by the evolution of information technology (IT). Typically IT and financial processes have evolved ahead of the assurance (audit) process. Assurance has lagged, stifled by the conservatism of its practitioners, obsolete regulations, and the lack of progressive social and economic forces. The emerging field of continuous auditing attempts to better match internal and external auditing practices to the reality of the modern IT-dominated environment in order to provide stakeholders with more timely assurance.

## *The real-time economy*

Businesses have been accelerating their activities in every possible domain attempting to achieve two interlinked objectives:

- Decreasing the cost of processes through automation; and
- Increasing the accuracy of processes.

Incorporating computers into business processes reduces manual processing and the costs of the associated human errors. Importantly, computerisation changes the intrinsic nature of these processes, requiring adjustments to the socio-technical structures of organisations.

The evolution of mainframes, microcomputers and, most recently, internetworking—using the internet for a wide range of business transactions—have provided the major drivers of business electronisation. However the real-time economy has mainly depended

[1] The author thanks QI Liu for her advice on this paper.

on the evolution of (i) sensing devices that automatically record economic events, (ii) enterprise resource-planning packages that integrate automated business processes, (iii) specialised business-reporting languages, and (iv) methods of integrating automated- and human-decision processes. Despite these developments, changes to business processes to more-effectively use technology are needed. These changes include business-process re-engineering and process reorganisation.

Continuous auditing represents a progressive shift in audit practices towards the maximum-possible degree of audit automation applied to the technological basis of the modern entity in order to reduce audit costs. The development of continuous auditing requires a fundamental rethink of all aspects of auditing, particularly in relation to:

- The way in which data is made available to auditors;
- The kinds of tests auditors conduct;
- How alarms triggered by audits are dealt with;
- The nature, frequency and direction of assurance reports.

The importance of some of these issues will only become apparent as continuous auditing is implemented. However, the auditing profession and other stakeholders need to start thinking now about the impact of continuous auditing when it is easier to guide this change rather than after systems have become established.

## Latencies

Four major types of latency (delay) are being reduced through the adoption of new technologies:

*Intra-process latency*: The time taken for a process such as updating accounts payable to be performed. These latencies are affected by the automation of process steps.

*Inter-process latency*: The time taken for data to pass between processes. These latencies are influenced by the adoption of interoperability standards such as XML (eXtensible Machine Language) which is a set of rules for encoding documents in machine-readable form. The financial value-chain will be substantially enriched when XML-coded transactions interact with XBRL (eXtensible Business Reporting Language) for general-ledger postings and, ultimately, the preparation of financial statements.

*Decision latency*: The time taken for a decision to be made, reduced to nanoseconds if decisions are made electonically. Auditors typically make a series of decisions based on errors detected in samples of populations. These human interventions take time. Rules can be developed to highlight automatically items for further examination or to accept samples as representative of the population.

*Decision-implementation latency*: The time taken for implementation of decisions, contingent on the nature of processes and the types of interconnections between

processes. Once a sample is deemed to need more examination, original documents must be retrieved for scrutiny and analysis. Automation can reduce this latency by automatically subjecting sub-samples to increased filtering and analysis.

### Elements of progressive automation

Starting with the giant US telecom, American Telephone & Telegraph Company (AT&T), over the last 25 years with colleagues I have worked on a plethora of projects aimed at increasing the timeliness of auditing and improving the quality of organisational data. This work has been undertaken primarily in conjunction with firms' internal auditors but sometimes with their external counterparts. These projects have generated a series of tentative conclusions about where we stand today, namely:

- Auditing needs to evolve to a radically-different methodology to satisfy the generic objectives of assurance and data integrity;
- Regulations governing the scope of audits are too narrow. The domain needs to expand, involving a reconsideration of the objectives of audits;
- The automation of audit processes is just one part of a wider set of economic, technological and process innovations;
- A new framework of assurance is evolving to incorporate more-advanced analytics, attempting to leapfrog the delay of assurance-technology in relation to business; and
- After scope and analytics, the two major changes impinging on audits are the timing and location of assurance work.

## Electronic measurement and reporting (XBRL)

XBRL, in both its general-ledger and external financial-reporting applications, although a very positive step towards automation, perpetuates some of the limitations of the 'paper-oriented' reporting model. To improve their social-agency function, audits should encompass corporate measurements and databases, not just financial statements. XBRL is a rigid model unsuitable for representing the interlinked fuzzy-boundary business organisations of today. However, the electronic assurance functions will be influenced by, and will influence the evolution of, XBRL.

Like most substantive regulatory-based changes, the evolution of XBRL has generated a series of unintended consequences including (i) pressure toward standardisation of reporting, (ii) facilitation of more-frequent reporting, and (iii) the standardisation of the semantics of accounting reporting. In some respects XBRL is a poor conduit to represent corporate transactions.

## Monitoring and control

Conceptually, the processes of measurement, monitoring, control, and assurance are tightly interlinked. Control typically focuses on the comparison of an actual value with a predetermined value to produce a variance or discrepancy. When the absolute value of a discrepancy exceeds a standardised amount, an alarm or alert occurs. Although extensive effort has gone into improving IT and, consequently, the measurement of actual values, there has been limited work into defining the models or standards that should be used under different circumstances, particularly when seasonality, growth-rates, business cycles and extraordinary events influence actual measures.

The proliferation of business processes and the ubiquity of technology and automation will not only change the minimum level of control from accounts (embodying multiple transactions) to individual transactions but will also require a different set of meta-controls to be enacted. These are part of the natural changes in business processes earlier discussed.

Two key considerations have been embedded in assurance regulations and procedures. First, the tradeoffs between the costs and the benefits of audits, leading to adoption of high-materiality thresholds considering today's technology. Second, the atomicity of controls and their observability, leading to most audit research being in the area of data audits not on the structures and compliance of controls.

The advent of the Sarbanes-Oxley Act in the US in 2002—which tightened financial reporting and audit requirements—propitiated a reconsideration of the latter which further emphasised management's accountability for control and accounting with assurers being clearly delegated to non-operational review roles.

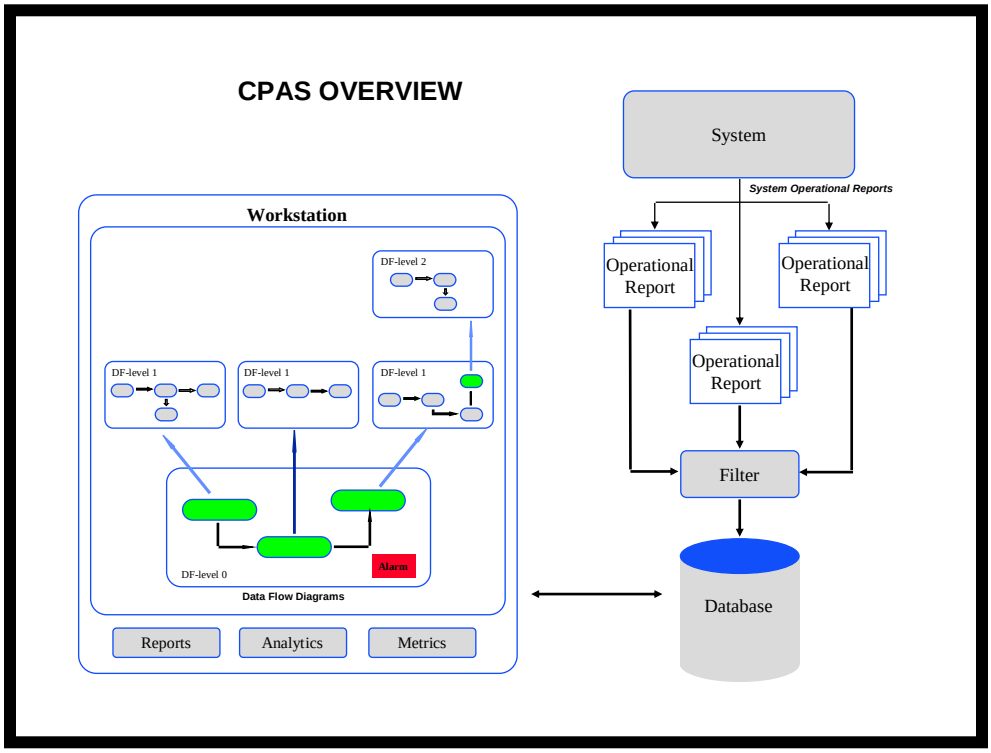
## *Continuous assurance*

The first recognisable examples of what today we call continuous auditing was our large-scale auditing system developed in the late 1980s at Bell Laboratories, the research arm of AT&T. That project relied on the pre-internet advanced information-technologies of the day (PCs, databases, corporate networks) to assure the reliability of the entity's billing systems through the automated acquisition and analysis of data and the electronic communication of alarms for the customer base of over 50-million households.

This system was designed to monitor and audit the billing system of AT&T in the context of the corporation's 'take back' strategy which involved billing clients directly rather than through operating companies. As the system was enormous and highly-sensitive, data extraction was through semantic processing in which electronic versions of reports were captured through a remote job-entry system and their content pattern-scanned for specific content. In **Error! Reference source not found.** a symbolic view of this system's architecture Figure 1 shows the system's electronic remote job-entry reports being filtered through semantic extraction procedures and placed in a relational database. This database was queried by screen-based reports that visually described the system in a 'flow-chart like' presentation comfortable to auditors.

Internal auditors, who intensively participated in the effort, were 'knowledge engineered' to acquaint them with the system and its audit rules. Past audit reports were also used to identify sources of data (metrics), types of analysis performed (analytics), comparative models (standards) and when alarms should be issued.

*Figure 1. CPAS Architecture*




This effort in actual data-monitoring to identify process flaws or data exceptions was originally denominated 'continuous audit' but today would be labelled 'continuous data audit'.

That first project demonstrated that the ultimate aim of continuous auditing is to bring auditing closer to operational processes, and away from the traditional backward-looking annual examination of financial statements. The CPAS project was eventually paralleled by the 'Prometheus' project that used its infrastructure to deliver information to billing managers analogous (but not identical) to the process-monitoring features of CPAS.

We progressively re-conceptualised continuous auditing with three main components: (i) continuous data-audit, (ii) continuous control-monitoring and 3) continuous risk-measurement and assessment.

## Continuous data assurance (CDA)

Continuous data assurance (CDA) uses software to extract data from IT systems for analysis at the transactional level to provide more-detailed assurance. CDA systems provide the ability to design expectation-models for analytical procedures at the business-process level, as opposed to the current practice of relying on ratio or trend analysis at higher levels of data-aggregation. Testing the content of an entity's data flow against such process-level benchmarks focuses on examining both exceptional transactions and exceptional outcomes of expected transactions. With such benchmarks, the CDA software can continuously and automatically monitor transactions, comparing their generic characteristics with predetermined benchmarks, thereby identifying anomalous situations. When significant discrepancies occur, alarms are triggered and routed to appropriate stakeholders.

Transaction verification is essential in most CDA implementations, especially in entities with disparate-legacy IT systems rather than single, integrated, enterprise resource-planning systems. When data is uploaded to a firm's data warehouse, potential errors that may be introduced to the data set have to be identified and removed before the data is suitable for automated testing. This step is undertaken by the transaction-verification component of a CDA system. Potentially, in a tightly-integrated enterprise environment with automated business-process controls, such data errors may be prevented by the client's resource-planning system.

Transaction verification is implemented by specifying data validity, consistency, and referential integrity-rules, which are then used to filter the population of data. These rules are designed to detect and remove two types of data errors:

> *Data-integrity violations*, including invalid purchase quantities, receiving quantities, and cheque numbers.
>
> *Referential-integrity violations*, largely caused by unmatched records among different business processes. For example, if a receiving transaction cannot be matched with any related ordering transaction, the indication is that a payment is being requested for a non-existent purchase order.

Examples of CDA include procedures for verifying:

- Master data;
- Transactions; and
- Key process metrics using analytics (including continuity equations)

For Itau-Unibanco (Brazil's largest financial institution) we have been developing a set of CDA endeavours that include (i) auditor branch-monitoring, (ii) transitory account-monitoring, and (iii) branch sales-analysis and monitoring. These endeavours are focused on detecting errors, deterring inappropriate events and behaviours, reducing or avoiding

financial losses and helping assure compliance with existing laws, policies, norms and procedures.

We have also worked with the audit-innovation team of consumer-products multinational Procter & Gamble in three projects, involving (i) identifying inventory problems at over 160 locations using key performance-indicators, (ii) examining worldwide vendor files and understanding vendor structures, duplicate payments and other issues, and (iii) automating the order-to-cash audit process on a stepwise basis. Latterly, we have concluded that continuous audit is a modular approach that finds the higher-automation return elements and focuses on their implementation.

## Continuous control monitoring (CCM)

The advent of the Sarbanes-Oxley Act and its assurance provisions on controls brought increased attention to the configurable nature of enterprise resource-planning controls. Continuous monitoring of business-process controls relies on automatic procedures, and therefore presumes that both the controls themselves and the monitoring procedures are formal or formalisable.

Working with German manufacturing conglomerate, Siemens AG, we made our first attempt to prototype control-monitoring which was followed by a more-complete audit-automation study. Currently, we are working on the formalisation of functions and their consequences upon separation of duties. This work has taught us about Siemens' audit action sheets (AASs) that detail step-by-step the review of their internal systems. In the Procter & Gamble audit-automation project, we created AASs as a first step when deciding which steps of the order-to-cash process to automate.

Among the lessons from the Siemens projects are that (i) enterprise resource-planning systems are very opaque, (ii) process- and control-rating schema are desirable, (iii) 20–40 per cent of controls may be deterministically monitored, (iv) perhaps another 20–40 per cent are potentially monitorable, (v) this CCM is a new form of alarm evidence that we do yet not know how to deal with, and (vi) continuous risk-management and assessment is needed for weighing evidence and choice of procedures

Examples of CCM include procedures for monitoring:

- Access control and authorisations;
- System configuration; and
- Business process settings.

Continuous data-assurance and CCM are complementary processes. Neither process is self-sufficient or comprehensive. Even if no data faults are found it cannot be concluded that controls are fail-safe. Further, even if controls are being implemented it cannot be assumed that data is totally trustworthy. However, in combination these monitoring approaches present a more-complete reliance picture. The financial crisis of 2007/08 and

the pressure of the Public Company Accounting Oversight Board (established in the US under the Sarbanes-Oxley Act) for 'risk based audits' encouraged us to conceptualise the Continuous Risk Monitoring and Assessment (CRMA) approach.

## Continuous risk management and assessment (CRMA)

In compliance with the Sarbanes-Oxley Act, management must monitor internal controls to ensure that risks are being adequately assessed and managed. Enterprise risk-management systems help companies identify and manage corporate risks. In compliance with Basel protocols, banks are required to assess their overall capital-adequacies in relation to their risk profiles. Regulators have encouraged financial institutions to validate their risk models to increase the reliability of risk assessments. The Accounting Oversight Board has exerted substantial pressures on audit firms to reduce audit costs through smarter use of audit procedures.

CRMA is a real-time integrated risk-assessment approach, aggregating data across different functional tasks in organisations to assess risk exposures and provide reasonable assurance on firms' risk assessments. CRMA include processes that:

- Measure risk factors on a continuing basis
- Integrate different risk scenarios into quantitative frameworks
- Provide inputs for audit planning

For the Itau Unibanco project we have been developing a set of risk indicators for the product sale cycle including four different banking products as well as a set of macro risk-indicators, all of which will be included into a normative risk-dashboard to be included as audit evidence to decide on the extent and scope of audit procedures. The CRMA area is still incipient and requires extensive thinking, experimentation and prototypes but we feel that will be a very important area of work

## *Future developments and constraints*

Our experience in over 10 corporate partnership projects has led to a belief that substantive changes are necessary to both measurement and assurance models. The same rules that helped to formalise and evolve the role of auditing in modern life now inhibit the evolution of many business-measurement processes, including assurance. These changes, forced by the progressive advent of the real-time economy, must be research-based, tested in practice, and then promoted and incorporated by standard setters.

The top priorities in assurance research should encompass creating:

- Control-system measurement and monitoring schemata including attempts at formalisation and structuring. This should include some form of control

representation and taxonomy, methods of quantification of control combinations, methods of incorporating the results of control-monitoring into quantitative assessment of control design and effectiveness;
- Standards for business-process monitoring and alarming;
- Automatic confirmation tools;
- A variety of modular audit bots (agents) to be incorporated into programs of audit automation; and
- Alternative real-time audit reports for different compliance masters

Complementary research needs include:

- Expansion of assurance to non-financial processes through continuity equations;
- Developing standards for continuous auditing; and
- Developing complementary assurance products.

Reconsideration of concepts and standards, particularly in relation to:

- Independence (which needs to be re-defined);
- The external-audit billing model which should be restructured to bill on function not hours;
- Audit firms improving their knowledge-collection and management processes to feed their analytical toolkits;
- Audit firms engaging in audit automation and pro-actively promoting corporate data -collection during the automation process
- Value–adding, which must be justified in terms of data quality; and
- Redefining the concept of materiality.

Miklos A. Vasarhelyi is KPMG Professor of AIS, Rutgers Business School Technology Consultant, AT&T Labs and editor of the *Artificial Intelligence in Accounting and Auditing* series.

## References

Alles, M.A., 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* (June): 137-161.
The Institute of Internal auditors, Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment, GTAG # 3, Altamonte Springs, Florida, 2005.
Vasarhelyi, M.A and M.L. Greenstein. 2003. Underlying principles of the electronisation of business: A research agend*a. International Journal of Accounting Information Systems* (March): 1-25.
Vasarhelyi, M.A. and F. Halper. 1991. The continuous audit of online systems. *Auditing: A Journal of Practice and Theory 10 (1): 110-125.*