Continuous Audit: Technology Enabled Continuous Assurance

‘Challenging Assumptions with Practical Experience’


from

‘The Vegas Sessions’

A White Paper authored by Dan French, Consider Solutions

6th March 2011
Introduction

‘Continuous Audit’ has been discussed and written about for decades. Conferences are run and books get written on the subject. But to this day, the definition is hard to pin down and there is quite a lot of semantic debate about what it is and is not. This debate is most fierce when exploring the perceived differences between Continuous Audit and Continuous Monitoring, of which more later . . .

A pretty classic view of Continuous Audit is that it is one of many tools used by Internal Audit to provide reasonable assurance that the controls in the business operational environment are suitably designed, established and operating as intended. The ‘continuous’ element of the label can refer to the frequency of testing throughout the year as opposed to end of year snapshots. Robert Mainardi wrote an interesting book on the subject entitled ‘Harnessing the Power of Continuous Auditing’ (Wiley).

A more contemporary view is that Continuous Audit is the application of automated tools to provide continuous assurance over financial or operational control and to check whether internal controls are functioning to prevent error and fraud.

But the world is moving on. Businesses are striving for global standardization, simplification and automation.

We are in an era where the core business processes are undergoing a transformation where the ‘factory processes’ that require no creativity or innovation are being consolidated into Shared Service Centers and even outsourced, supported by a common process and system and template that is typically implemented in large scale ERP software from providers such as SAP or Oracle. These transformed processes and support organizations are often set up in geographically separate locations to benefit from labor arbitrage and cost efficiencies and to support global time zones and languages. These centralized service units also require strong control and exception management systems.

The control systems of the past were largely ‘proximity controls’, by which I mean the control implied by co-located process execution and oversight. It is not long ago when the implied control over expenditure was that the financial controller personally approved all high value purchases and the person requesting the purchase and their role was well known to the controller, and usually resided in the same building. These ‘proximity controls’ were rarely written down, but effective. They typically completely break down as a result of finance transformation.
The new world requires an approach to audit (and indeed to management) that recognizes the inherent complexity and volume associated with today’s global processes. Major organizations today are looking for a better way to assure their businesses run ‘as advertised’ and to avoid any issues that could cause reputational damage.

Despite the wide disparity between definitions, widespread application of Continuous Audit remains elusive. 32% of organizations recently surveyed by the Institute of Internal Audit (IIA) reported that they perform continuous auditing. In another recent survey by PriceWaterhouseCoopers (PWC) 81% of companies ‘aspired to’ continuous auditing.

Challenging Our Assumptions

One of the big questions that has been raised about Continuous Audit and indeed its sibling, Continuous Monitoring, is WHAT should be monitored.

But before we get to that, let’s answer the question WHY we would want to monitor! This is an important question at the heart of some potentially dangerous assumptions.

The widely held view is that internal audit should assess the effectiveness of the internal control system by validating that it is suitably designed, established and operating as intended. This can lead to some interesting results best illustrated by the winter picture below.

![Winter Picture](image.jpg)
This is a lovely illustration of difference between risk and control, which becomes clearly visible with monitoring technology (snow in this case!).

The entrance to the car park facility in this photograph has a state of the art control system, an automatic barrier that opens only when you swipe your employee identity card on the reader and only lets one car through at a time. Similarly on exit, the driver swipes their identity card again, the barrier opens, the car drives out and the system records that the employee has left the premises and the car is no longer their liability. This way, it is clear that only authorized people can use the facility and that a record is kept of each visit. The automated control works perfectly and as designed. However, the tyre tracks in the snow illustrate how people get round the control, and that the real risk of unauthorized car park usage is not effectively addressed. This is an important consideration when we look at continuous audit.

Interestingly, the IIA defines internal auditing as ‘an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes’.

This is a very ‘outcome oriented’ definition and focuses on the EFFECTIVENESS rather than purely EXISTENCE.

A Continuous Audit approach should challenge the existing controls framework for two reasons. Firstly, the underlying assumptions about how the controls mitigate the risk are often ‘flaky’ at best. Secondly, Continuous Audit, which is based on tests that are COMPLETE, CONSISTENT and CONTINUOUS, can remove the need for some standard control tests. When you are checking 100% of controls and the data, it is quite common for 2 or 3 CA tests to replace a larger set of tests which may have evolved over time to counterbalance the vagaries of sample based testing.

**Insights on Risk and Complexity**

There is no doubt that increases in business complexity and risk go hand in hand. A glance at the origins in mortgage backed securities of the 2008-9 global financial crisis is a testament that. At the same time, businesses are developing an increasing sensitivity to company reputation as well as financial performance. Thirdly, the increased scrutiny and penalties on bribery and corruption (think FCPA and UK Bribery Act) is reinforcing the message that ‘ignorance is no defence’ to accusations any longer. These factors are driving the new breed of audit committee members, executives and audit and risk professionals towards best practices in risk management and assurance. Continuous Audit is one of these best practices. It is no surprise that market segments where reputation can be most delicately affected are leading the charge (think pharmaceuticals,
capital equipment, consumer goods, financial services et al). From our work with organizations in the US, Europe and Asia, three key insights have emerged in this area.

1. **Standardization & Simplification CREATE complexity – deal with it!**
   The standardization & simplification agenda is ongoing at all big organizations as referred to earlier. What we have observed, somewhat counter-intuitively, that as the external ‘interface’ to processes and technology becomes more standard and simple, the internal complexity tends to increase. Consider the humble motor vehicle below, captured on camera in Manila. This is a very non-standard vehicle, highly customized Manila ‘jeepney’. Despite the fact that all the jeepneys look different, if there is a mechanical problem the driver can get under the hood and fix the issue.

   ![Humble Motor Vehicle](image)

When you look a contemporary, state of the art vehicle such as the BMW below, there is a high degree of standardization for the driver and for the manufacturer. It is efficient to produce and efficient to drive. But in the unfortunate event of any mechanical or electronic issues, the driver is lost without a specialist with the right equipment.
Look at the Apple iPhone, the pinnacle of user centric design (OK, that’s the iPad, but bear with me!). This beautifully engineered, standardized, simplified device cannot be customized, but the components are constructed and assembled by 9 companies in 6 countries. Any problem with the device, you have no chance of fixing it.

In the same way, modern business systems such as ERP present a unified view of a process across plants, divisions and legal entities through a highly standardized process template and interface for the business users. But that simplicity hides a complex set of internals, including the elements we rely on for controls. The mechanism for designing and implementing controls are complex in these environments and the permutations of usage are enormous. Five years ago the SAP R/3 ERP system had 55 thousand options for executing business transactions, and it is getting more complex as each year and upgrade goes by.

2. The Systems Myth – the System is NOT the Process

Organisations have invested massively over the years in integrated systems to achieve process standardization, global integration, business efficiency and economies of scale. Much of this has been driven in recent years by the finance transformation agenda for simplification and standardization that enables shared services.

A great deal of value has been achieved, in part by forcing the organization to take decisions to ensure harmonization. The devil is in the detail of course, and many businesses have a standardized process on paper but in the heat of ERP implementations some of the planned standardization gets lost, and this additional complexity can remain invisible to management until the bright light of continuous monitoring shows the truth.
The reality today is that in most businesses enterprise systems have been the catalyst for a standard data input process, not a standard business process. Management is told that we have embedded ‘controls’ in our systems that ensure business controls will work and associated risks mitigated. It is true up to a point, but only up to a point and there is often a lack of clarity on where that point is!

Consider this, a classic business process with a well understood accounting control, the three way match between deliveries (Goods Receipts), Purchase Orders and Invoices/Payments. We all know the standard business best practice here which aims to ensure that only what has been genuinely purchased gets paid for, purchases are approved in advance and expense can be predicted.

There is in most systems an automated way of setting this ‘control’, to only allow a GR note if a PO exists. So, a delivery is made to a plant or a consulting invoice to a manager at head office. No purchase order exists. The recipient calls their contact to get a PO raised. The PO gets raised in the system. Then the recipient of the goods or invoice can post their acceptance and the invoice matching and payment process kicks off. The system is happy that the sequence of events is correct and meets the embedded ‘control’. From a business perspective, it’s a mess. The system is NOT the process.

**Standardized process control**

ERP is configured to only allow GR if PO exists, however...

1. Truck drops off shipment, but no PO exists
2. Warehouse worker calls up purchasing to create a PO
3. Purchasing creates PO for Shipment
4. GR is created against PO

“The myth of automated controls in systems”

The embedded system controls are good, but not sufficient to address certain key risks. So how do we address this issue?
Automated, embedded configuration controls in systems such as ERP are very important and should be used to an appropriate level for the business. But every preventive control has ‘workarounds’ as illustrated above. The tools to implement these configuration settings are technical and error-prone and consequently are not always consistently set where management believe they are.

To complement the appropriate preventive configuration controls, effective continuous monitoring should be applied to key risk areas. Continuous Audit should be used to monitor the configured controls themselves (are they set where we think they are, for all vendors/materials etc, have they been changed?). In addition, Continuous Audit should also alert to changes to master data and transactions that fall outside expected risk norms.

3. It’s NOT about controls, it’s about RISK!

There is a lot of focus on establishing control frameworks reporting on the existence and operation of controls. This is a good start and is both established practice and a regulatory requirement in many jurisdictions.

However, every control is based on some assumptions, and too often the assumptions get lost in the development and implementation of the control framework. The example above is a classic case. We need to complement our controls thinking with ‘what is the underlying risk’ and how we address that.

I can no longer count the times in our work where the controls are perceived to be implemented AND effective, only to find (under the bright lights) that the ERP controls are not implemented for all vendors (or customers, materials etc) AND the shadow process I described above is alive and well, undermining management’s drive for a common, controlled process. To paraphrase a former US presidential candidate, ‘it’s about the risk!’.

Continuous Audit and Continuous Monitoring

In today’s business environment, the essence of both Continuous Audit and Continuous Monitoring is to provide a radically improved level of assurance on operations and financial reporting (and anything else you want to continuously monitor!).

But what is the difference? There is quite a debate on the web forums on this topic, especially the use of the term ‘Continuous Controls Monitoring’ (CCM). Frankly, this is mostly a debate about semantics. And whilst the semantics could benefit with some cleaner terms and definitions, the key issue is for organizations to focus on their objectives and to implement processes and
methodologies that will help them in that journey. The key difference between the two, in my experience, is the stakeholders and associated details of the end to end process. So, Continuous Audit is about INDEPENDENT ASSURANCE for the AUDIT stakeholders and thus the company. Continuous Monitoring or Continuous Controls Monitoring is for MANAGEMENT (typically led by the CFO and the Finance function) to assure the business is running effectively and efficiently (and perhaps legally!).

To achieve a high level of assurance for either group of stakeholders requires consistent, complete and continuous testing:

- Consistent in that the risk or control needs to get the same degree of testing wherever it is located, head office or far flung subsidiary. US domestic or Europe, system 1 or system 2, SAP ERP or Oracle ERP (you get the picture . . )
- Complete in that we can no longer rely on statistical sampling. We need to test 100% of the controls or risk activities that are in scope, i.e. rated as a priority. Only then can we avoid the misunderstanding that so often occurs at Audit, Compliance and Risk committees. To be told that 90% of the key controls have been tested and proven to be effective when in reality 0.001% of revenue has been tested through sampling, is understandably ambiguous!
- Continuous in that the testing should be ongoing so that exceptions can be highlighted and dealt with close to the event rather than at Quarter or Year end. Whether ‘continuous’ means daily, weekly or monthly depends largely on the objectives of the program and the stakeholders and end to process for addressing exceptions identified.

Clearly automation is a pre-requisite for this level of audit or monitoring. It would be difficult and highly costly to try to perform such tests manually given the sheer volume of activities on a day to day basis across locations, regions, legal entities, business segments and varying systems.

The influential technology analysts, French Caldwell and Paul Proctor of Gartner Group, produced an interesting model to define the dimensions that need to be monitored to achieve this objective. It is a useful checklist for 360 degree control and risk testing. In summary these dimensions are;

- Access to system functionality, to monitor segregation of duties, critical combinations and sensitive access – ACCESS RISK
- Application configuration, to monitor the presence, appropriate configuration and modification of built-in embedded application controls such as the three way match controls described earlier – CONFIGURATION RISK
• Master or static data, to monitor key or suspect changes or duplication to the critical static data that drives processes in enterprise systems. Often the cause of other transaction related issues such as duplicate payments – MASTER DATA RISK
• Transactions, to monitor the individual business events recorded in enterprise systems for risk management and performance improvement purposes – TRANSACTION RISK

There is a question as to why testing the integrity of business transactions is relevant to controls. True, the control system should be independent of the activities themselves. However, as discussed earlier, the question is about RISK not just CONTROL.

It is true that just because transactions are "correct" doesn't mean that controls are in place or operating. However, just because the controls are in place and operating doesn't mean the underlying risk has been mitigated either.

The question relates to whether the controls are not just working, but EFFECTIVE. Experience indicates that there is too much assumption that textbook controls actually achieve the desired effect.

There is clearly a case for both monitoring controls AND data and transactions. They are all important techniques and essential for both CONTINUOUS AUDIT and CONTINUOUS MONITORING. These techniques can identify if the controls are in-place and working AND identify if the controls are effective (i.e. mitigating the risk / undesirable activity). The first is achieved by monitoring the 'control' and latter by monitoring the data and transactions. The focus is in finding EXCEPTIONS to accepted risk or performance tolerances.

Continuous Audit and Continuous Monitoring should target 360 degree testing and 100% coverage consistently, completely and continuously. The diagram below shows an example of what we mean by 360 degree coverage;
360’ Coverage for KEY Risks

**ACCESS RISK**
- Detect Segregation of Duties for Purchase Order creation vs. Goods Receipt

**MASTER DATA RISK**
- Detect vendors with no material pricing set

**TRANSACTION RISK**
- Detect Good receipts with same posting date as Purchase Order

**CONFIGURATION RISK**
- Detect vendors where GR/IR not set

Essentially, Continuous Audit and Continuous Monitoring find exceptions that just don’t typically get found through sample based testing or ad hoc analytics, for example;

- Duplicate payments
- Payments without purchase orders
- Unbilled revenue
- Inappropriate changes to vendor bank account details
- Changes in payment terms or prices on specific orders
- Approvals to unusual vendor or customer master changes
- Customer credits just below approval limit
- SoD checks at the individual level e.g., POs created and released by same person, GR created by same person as approved the PO.
- Deliveries with no reference to a Sales Order
- Over deliveries
- Sales Orders for Customers over Credit Limit
- ‘Unusual’ GL postings
- Multiple PO’s to avoid signoff limits
- Nominal value PR’s to ‘make the process work’
Properly applied and with an appropriate end to end process, CONTINUOUS AUDIT highlights exceptions to expected business practice, whether in the areas of risk, fraud and waste.

**Audit as a business partner – Assurance AND Guidance**

The new realities of the business environment create a mandate for the forward looking internal audit department to provide both independent assurance AND best practice advice to management on performance optimization. ‘Compliance’ is no longer the primary business driver, it is Business Excellence. Internal Audit has a powerful role to become a true business partner to management in offering opportunities for performance improvement, process change and control optimization as well as risk assessment and assurance.

New opportunities emerge with Continuous Audit. Automation and 100% testing on a 360 degree horizon allows the organization to take advantage of some key insights. Every key risk indicator (KRI) has a mirror image key performance indicator (KPI). Think about it.

Consider the risks in the Accounts Receivable function. The key risks are ‘not getting paid’ and booking revenue for sales which do not meet accounting rules. As a result we implement controls and monitor activities around credit checks for new customers, non-standard payment terms and delivery performance (quality, quantity, timeliness). Interestingly the KPI is typically Days Sales Outstanding (DSO). It is standard accounting practice to monitor DSOs, and if the target is 42 days, and the average DSO moves to 45 days, frenzied activity ensues in the accounting function. Continuous Audit and Continuous Monitoring allows us to support the business in new ways. Rather than a frenzied collections activity, we can monitor the factors that typically impact DSO. What are they? These factors are typically incomplete or incorrect customer master data, incomplete customer Purchase Order data, non-standard payment terms and delivery performance. Sound familiar? Using these contemporary approaches we can support business management ‘ahead of the curve’ to not only drive business performance, but to ASSURE it.

There needs to be a delicate separation between assurance and guidance but, with the right leadership and relationship management skills in the internal audit function together with appropriate methodologies, there is a great opportunity to drive business performance and assurance to new levels.

**Continuous Audit and Continuous Monitoring Approach & Best Practices**

This is a change journey not a one-off project. There is a great deal of learning along the way, not just about how to monitor, but what to monitor and why, how to deal with the results and
how to measure progress.

Best practices fall into three categories; program management and execution, change management and executive visibility;

Program Management & Execution

- It is a cross functional program – have a strong relationship oriented program manager with good executive support
- Consider organisation, process, people and technology
- Use an initial ‘pathfinder’ project on narrow risk and geography focussed scope to educate and build stakeholder commitment, as well as inform the broader plan
- There is an important technology component, but don’t let it become or be seen as a technology project
- Prioritize based on risk and suitability for automation
- Iterative refinement of rules/tests, process and scope. Deploy ... use ... learn ... review ... refine ... extend.
- Review current practices at all stages. Is there a better way, can we re-engineer our test plan?
- Take the opportunity to engage & connect to help drive partnership with business units
- Offer performance improvement opportunities as well as risk assurance

Change Management

- Communicate
- You need active engagement from key stakeholders in Audit, Finance, IT, Applications and any other business functions in scope (e.g. procurement)
- You need a clear vision, with buy-in, first steps, committed stakeholders and a plan
- This is a change initiative not a one off project – treat it as such
- It is not just an internal change management task, your external auditor is a stakeholder on the journey too! Consider how and when you involve them.
- Use an initial ‘pathfinder’ project on narrow risk and geography focussed scope to educate and build stakeholder commitment, as well as inform the broader plan
- Educate executive sponsors continually – no surprises
- Ensure everyone understands that however world class the organisation is, you will find a lot of exceptions. That is a good thing. They were there yesterday, but no-one knew
- The process challenges assumptions, answers some questions and raises new ones – build time in the plan for this
• Work through the end to end process and refine as you go. How do we manage the exceptions we find? Who owns them? What is expected?
• Recognise that some resistance is natural – accept it, it may be related to formal or informal performance measures – understand it
• No recriminations for lack of previous visibility of control failures
• Avoid measurement and comparison in the early stages
• Encourage recognition of the fact you have moved the inspection ‘microscope’ from 1x to 1000x magnification. You will find issues.
• Keep communicating the vision and the steps you have achieved
• Communicate

Executive Visibility

• Get sponsorship as high as possible – CFO or Audit Committee, preferably both
• Have an active steering committee that regularly meets
• Take time to educate, discuss and explore the assumptions you are challenging about the risk, control and systems environment
• Ensure the vision is agreed and be clear this is a program not a ‘project’
• Set, meet and report realistic goals
• Communicate challenges
• You need a clear vision, with buy-in, first steps, committed stakeholders and a plan
• Develop an effective executive reporting and communication tool, such as Balanced Scorecard – what are the measures of progress and success?

The narrow path or pathfinder project at the outset, used to explore what is possible and to inform the vision, business case and plan, is essential. The following diagram illustrates the concept;
The best practice approach for the overall program includes the following work streams;

Best Practice Approach

- CM/CA Test Definition & Optimization
- IT Planning & Operability
- Information Dissemination & Exception Action Planning
- Pilot “Business As Usual” on Narrow Path Scope
- Assess & Confirm Business Value Achieved
- Skills, Competency & Best Practices Development
- Roll-Out & Follow-On Planning

Although some organizations resist the idea at first, it is good to engage your external auditor early and often throughout the process. They will benefit from an effective program also. It will save them effort in audits (as well as save you money), it will change the nature of elements of
their audit plan, remove some of the low level work that their staff dislike and provide a more challenging and innovative working environment for their teams. They also are part of the change process and their support can help accelerate elements of the program.

The Value of Continuous Audit and Continuous Monitoring

The new generation of Internal Audit department is run by a Chief Audit Executive (CAE) whose vision and purpose for audit is to provide cost effective risk assurance for the business AND provide advice and guidance to management.

The value is clear at a number of levels;

- Providing more effective and efficient Risk Assurance for business operations
- Providing comprehensive validation for the effectiveness of the internal control system
- Supporting effective decision making for business performance improvement

In considering the business case for Continuous Audit or Continuous Monitoring, the following factors are critical;

1. Be very clear on the mission and objectives for the program – what does success look like?
2. Understand what is achievable with the process and technology
3. Have a clear view of the tasks and effort required to achieve the objectives
4. Ensure you have appropriate expertise to support your program in planning, execution and skills transfer to your own organisation

This is a new journey for most organizations and, as the saying goes, ‘the road to hell is littered with good intentions’. To maximize your chances of success in achieving your objectives, it is crucial to conduct a ‘proof of concept and value’ project on a narrow path scope in a limited time period to confirm and provide business case input to the four critical success factors above. Demonstrate some of the effort savings and improvements during this early process.

Subsequently, a realizable business case can be developed based on practical experience. Typically business cases conform to specific organizational norms but the benefits to be articulated and quantified should include at least the following;

- The overall vision and rationale
- Tangible benefits of Continuous Audit/Continuous Monitoring
Cost savings AND cost avoidance through reduced effort and external fees, including:

- Internal Audit Effort
- External Audit Effort
- Finance Effort (centrally and locally (often disguised!))
- IT Effort
- Other external effort (e.g. outsourced audit issue remediation, duplicate payment recovery etc)

- Improved risk management – 100% testing, 360 degree coverage, control validation
- Enhanced decision support for performance improvement

For many organizations, the value of enhanced assurance on operations, financial reporting and reputation is more than sufficient to make the case for a net neutral business case over three years. A key point to remember is that if this level of enhanced assurance is required (based on 100% coverage, 360 degree testing), the effort and cost of performing this without a new approach would be both extremely high in staff costs and unmanageable.

Summary & Conclusions

The new generation of Internal Audit department is led by a Chief Audit Executive (CAE) whose vision and purpose for audit is to provide cost effective risk assurance for the business AND provide advice and guidance to management to help drive performance improvement.

Continuous Audit and Continuous Monitoring require technology, but they are not technology projects, they are business change programs. Engage experts in all the fields but invest heavily in communication, relationships, vision building and progress reporting.

This is no longer the era of ‘check box’ auditing. Continuous Audit and Continuous Monitoring make a big contribution to the new realities of Internal Audit.