consider

solutions for world class finance

Flawless Finance:

The Role of Continuous Controls Monitoring & Continuous Transactions Monitoring in Your Organisation

Developing and implementing financial controls is only effective when those controls are tracked to ensure they operate as designed and that business transactions are processed as prescribed. This whitepaper explores the concept of Continuous Controls Monitoring (CCM) and Continuous Transactions Monitoring (CTM) and details how these strategies can help your organisation address the detective, preventive, and even predictive nature of data analytics in finance processes. Read this white paper and find out more about:

- The importance of Continuous Controls Monitoring
- How to validate that your controls exist and are effective in managing risk
- How CCM can improve shared services organisations
- How CCM can help avoid issues that could cause reputational damage
- Approaches for automating control processes for maximum business value
- A new model and checklist for 360-degree control and risk monitoring

infor Gold Channel Partner

CONTENTS

Introduction & Recent History

'Continuous Monitoring' of financial and operational processes has been discussed and written about for some years. Continuous Monitoring (CM) is a detective, preventive and even predictive data analytics-based feedback mechanism used by management to ensure that internal financial controls operate as designed and that business transactions are processed as prescribed. This monitoring method is the responsibility of management and can form an important component of the internal control structure. A subset of Continuous Monitoring focused solely on monitoring existing control operation is termed Continuous Controls Monitoring (CCM). The term used for the subset that is focused on the monitoring of business transactions and data for evidence of control effectiveness, broader risk assurance or performance management, is termed Continuous Transaction Monitoring (CTM).

The generally accepted purpose and target benefits of Continuous Monitoring are as follows:

- Enhanced and more timely oversight of compliance across the enterprise
- Improved efficiency and effectiveness of the control environment through automation, leading to cost efficiencies and allowing the reallocation of resources
- Business improvement through reducing error and waste by exception identification and remediation that streamlines processes
- Elimination, prevention & detection of other key risks, which may not be material from an ICFR (Internal Controls over Financial Reporting) perspective, but which are still critical to the organisation such as fraud, bribery, corruption, inappropriate payments etc.
- The ability to report more comprehensively on control effectiveness and compliance both internally and with external bodies, thus helping to reduce audit fees and internal co-ordination effort

As well as a focus on reducing the cost and improving the depth of risk management, the past couple of years have seen a growing focus on business efficiency and effectiveness gains through enhanced standardisation, simplification and automation in global processes.

We are in an era where the core business processes are undergoing significant transformation. Common processes, such as transactional finance, HR, Procurement and IT, are being consolidated into Shared Service Centres and get supported by a common process template that is typically implemented in large scale ERP software. These transformed processes and support organisations are often set up in geographically remote locations to benefit from labour arbitrage and cost efficiencies, skills availability and to assist global time zones and languages. The centralised service units also require strong control and exception management systems given that the new end-to-end processes are no longer under the one span of management visibility, responsibility or control.

The control systems of the past were largely 'proximity controls'. Process execution and management oversight were co-located. It is not long ago that the implied control over expenditure meant that the local financial controller personally approved all high value purchases and the person requesting the purchase 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 organizational, process and system changes inherent in finance transformation. While the controller may still own the responsibility, his/her ability to exercise oversight has reduced. Consequently, and also as a result of corporate governance regulations, we have implemented stronger, more objective control systems, but as we will see below, they do not necessarily instill the confidence that we might hope.

The new world requires a Continuous Monitoring approach 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 through unexpected, incomplete or inappropriate critical activities.

Challenging our Assumptions

One of the big questions that have been raised about Continuous Monitoring is 'WHAT should be monitored?'. But before we get to that, let's answer the question 'WHY we want to monitor?'. This is an important question at the heart of some potentially dangerous assumptions. The widely held view is that management 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.

This is a good illustration of the 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 authorised people can use the facility and that a record is kept of each visit. The automated control works perfectly and as designed. However, the tire tracks in the snow illustrate how people get round the control, and that the real risk of unauthorised car park usage is not effectively addressed. The car park may not be a critical or 'key' risk, but it does perfectly illustrate a broader problem. Think of the 'control' represented by the barrier in the previous image and 'the transactions' represented by the tire tracks. We need to continually validate that our controls exist AND that they are effective in managing the risk.

This is an important consideration that illustrates why our Continuous Monitoring approach must include both Continuous Controls Monitoring (CCM) and Continuous Transaction Monitoring (CTM).

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 of the mortgage backed securities that became instrumental in the 2008-9 global financial crisis is a testament to that. At the same time, businesses are developing an increasing sensitivity to company reputation as well as to financial performance. Thirdly, the increased scrutiny and penalties on bribery and corruption (think FCPA and the UK Bribery Act) are reinforcing the message that 'ignorance is no defence' with respect to illegal activity conducted by employees. These factors are driving boards of management to implement best practices in risk management and financial assurance. Continuous Monitoring 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 organisations in the US, Europe and Asia, three key insights have emerged that contribute to the case for Continuous Monitoring.

1. Standardisation & Simplification CREATE Complexity

The standardisation & simplification agenda is ongoing at all big organizations as referred to earlier. What we have observed, somewhat counter-intuitively, is 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, highly customised Manila 'jeepney'. Despite the fact that all the 'jeepneys' look different, if there is any mechanical problem, the driver can get under the hood and fix the issue.

When you look at a contemporary, state-of-the-art vehicle such as the BMW above, there is a high degree of standardisation 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 also at the Apple iPhone, the pinnacle of user centric design (OK, that's the iPad, but bear with me). This beautifully engineered, standardised, simplified device cannot be customised and its 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 globally unified view of a process across plants, divisions and legal entities through a highly standardised 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. For examples, five years ago the SAP R/3 ERP system had 55 thousand options for executing business transactions, and it is getting more complex with each year and upgrade that 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 standardisation, 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 standardisation that enables shared services.

A great deal of value has been achieved, in part by forcing organisations to take decisions to ensure harmonisation. The devil is in the detail of course, and many businesses have a standardised process on paper but in the heat of ERP implementations some of the planned standardisation gets lost. 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 processes will work 'as advertised' consistently and with associated risks mitigated. This is true 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 costs can be predicted.

There is in most systems an automated way of setting this 'control', to only allow a Goods Receipt (GR) note if a Purchase Order (PO) exists. So, a delivery is made to a plant or an invoice for services delivered to a manager at head office. No purchase order exists. The recipient calls their contact to get a PO raised. The PO gets raised and approved 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.

This validation of the true process execution is a classic use-case for Continuous Monitoring.

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

Truck drops off shipment, but no PO exists

Warehouse calls up Purchasing to create a PO

Purchasing creates PO for Shipment

GR is created against PO

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 earlier. The tools to implement these configuration settings are technical and error-prone and consequently are not always as consistently set as management believe they are. To complement the appropriate preventive configuration controls, effective continuous monitoring should be applied to key risk areas and should be used to monitor the configured controls (CCM) themselves (are they set where we think they are, for all vendors/materials etc., have they been changed?). In addition, Continuous Monitoring should also alert to changes to master data and transactions (CTM) that fall outside expected process and control 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 3-way match example above is a classic case. We need to complement our controls thinking with 'what the underlying risk is' and how can we address that.

I can no longer count the times in our work where the controls are perceived to be running effectively, only to find (under the bright lights) that the ERP controls are not implemented as management believe. For example, for all vendors (or customers, materials etc.), 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!'.

The Role of Continuous Monitoring

To achieve the level of assurance that management and shareholders are looking for in our increasingly complex world requires *consistent*, *complete* and *continuous* testing/monitoring:

- *Consistent* in that the risk or control needs to get the same degree of testing wherever it is located, at head office or far flung subsidiary, US domestic or Europe, system 1 or system 2, ERP A or ERP B.

- *Complete* in that we can no longer rely on statistical sampling. We need to test 100% of the controls and risk activities that are in scope, i.e. rated as a priority. We want to KNOW that our controls are working. 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 closer to the event rather than at Quarter or Year End. Whether 'continuous' means daily, weekly or monthly depends largely on the objectives of the stakeholders.

Clearly automation is a pre-requisite for this level of 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 monitoring.

In summary these dimensions are:

- Access to system functionality, to monitor segregation of duties (SoD), 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 exceptions in the individual business events recorded in enterprise systems for risk management and performance improvement purposes – TRANSACTION RISK

There is sometimes 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.

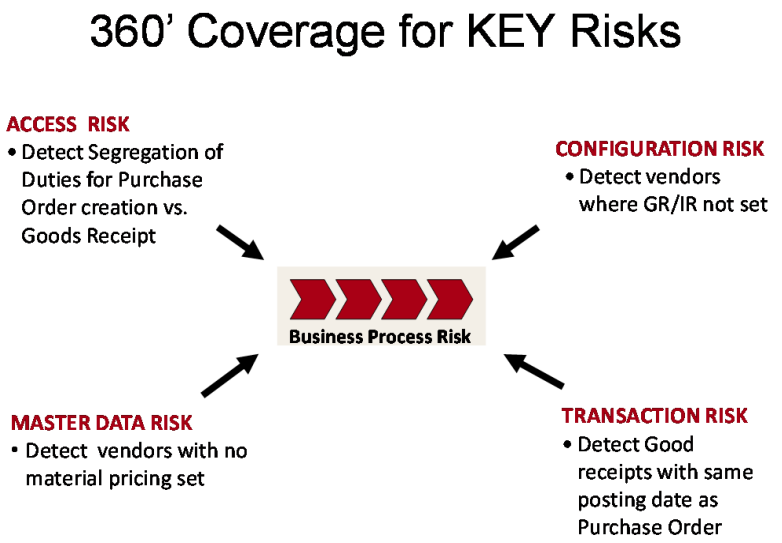
It is true that, just because transactions are 'correct', it doesn't mean that controls are in place or operating. However, just because the controls are in place and operating, it doesn't mean the transactions are correct or the underlying risk has been mitigated as illustrated in the car park image. 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 need to monitor both controls (CCM) and transactional data (CTM). These techniques can identify if the controls are in place and working AND identify whether the controls are effective (i.e. mitigating the risk/undesirable activity). The first is achieved by monitoring the 'control' and the latter by monitoring the data and transactions. The focus is in finding EXCEPTIONS to accepted risk or performance tolerances.

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:

Essentially, Continuous Monitoring finds 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 (POs created and released by same person, GR created by the same person who 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'

New opportunities emerge with Continuous Monitoring. 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 this . . .

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 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?

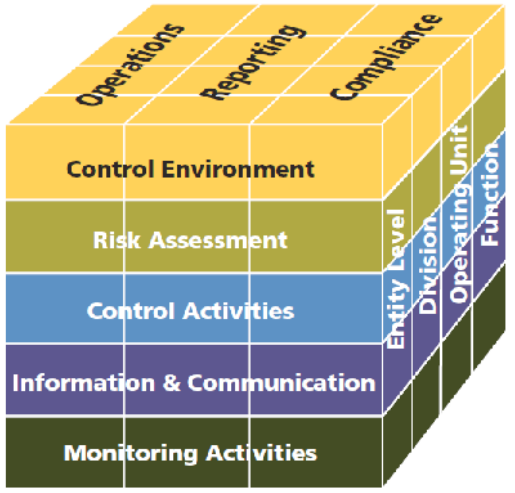
These factors are typically incomplete or incorrect customer master data, incomplete customer Purchase Order data, non-standard payment terms and delivery performance. Sound familiar? Using these contemporary approaches we can support business management 'ahead of the curve' to not only drive business performance, but to ASSURE it.

Properly applied and with an appropriate end-to-end process, Continuous Monitoring highlights exceptions to expected business practice, whether in the areas of error, fraud, waste and even business performance.

COSO 2013 and New Opportunities for Continuous Monitoring

It is timely to be discussing approaches to financial risk and control now. The basis of Sarbanes Oxley and other financial reporting regulatory and corporate governance requirements is the Committee of Sponsoring Organisations of the Treadway Commission (COSO) framework. The 2013 revision of the COSO framework, which is targeted for implementation by end 2014, requires organisations to review their systems of internal controls and address opportunities for improvement and optimisation. This period of review plays directly to the opportunity and business case for Continuous Monitoring.

Overview of the revised COSO framework - the 'cube'



For more details on the opportunities for improvement you can see a summary entitled '5 Opportunities: Financial Control Best Practice with COSO 2013' at http://bit.ly/1le9wrV with a link also to the more detailed White Paper on the topic.

Summary & Conclusions a.k.a 'Hits & Myths'

- We have a 'perfect storm' of increased stakeholder expectations on financial control & assurance and a compliance-led (COSO) drive to review systems and methods of internal control.
- Big data analytics have executive attention on the revenue and customer side, and this attention should be reflected into the core finance processes for driving efficiency, effectiveness and good governance here.
- Increasing simplification, standardisation, globalisation and automation of finance processes disguises hidden complexity that needs a new approach to process and risk assurance.
- Global ERP system controls are no substitute for vigilance for the unexpected or out-of-policy tire 'tracks'.
- Process optimisation and the drive for process excellence requires new methods for identifying and addressing process variation
- The case for action for Continuous Monitoring of finance processes has never been better.

consider

solutions for world class finance

About the Author

Dan French is CEO of Consider Solutions, a firm that provides business solutions and consulting services to help organisations on the journey to World Class Finance. The firm applies management advisory and technology capabilities focused on finance process optimisation, risk management and reducing the cost of compliance, control and assurance. Consider Solutions' methodologies deliver rapid, cost-effective results whilst providing the flexibility required by business management.

Dan has run the firm for 12 years and has a background of 25 years in general management, performance improvement, process change and technology. Dan advises organisations in Europe, US and Asia on strategies for continuous monitoring and exception analytics. Dan claims to live in London despite his travel schedule. He can occasionally be observed playing blues guitar or sampling fine red wines, but rarely at the same time for reasons of practicality rather than preference. Dan can be contacted at dfrench@consider.biz

If you want to learn more on this topic or would like to benchmark your own organizations current situation and vision against leaders or your peer group, contact Consider Solutions at www.consider.biz

infor Gold Channel Partner