A Practical Approach to Continuous Controls Monitoring

David Vohradsky, CGEIT, CRISC, is an independent consultant with more than 30 years of experience in the areas of applications development, program management and information risk management. He has previously held senior-level management and consulting positions with Protiviti Inc., Commonwealth Bank of Australia, NSW State Government, Macquarie Bank, and Tata Consultancy Services. Vohradsky is a member of ISACA's CRISC Certification Committee. He can be contacted at *davidvoh9@gmail.com*

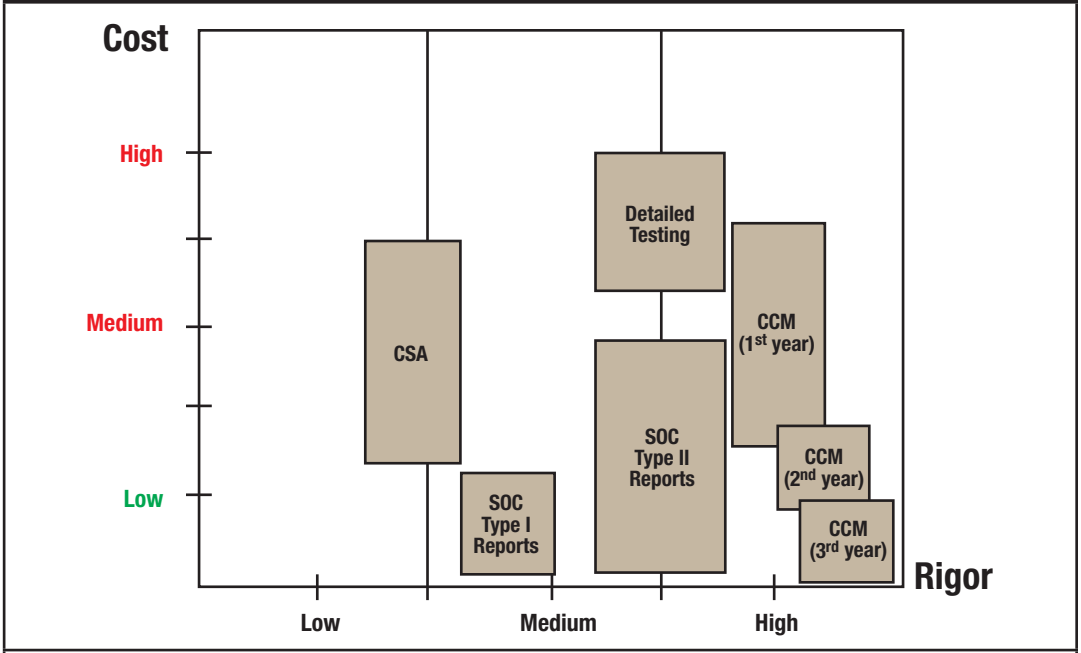
One of the responsibilities of line management in many organisations (particularly in financial services) is to provide assurance to the chief executive officer (CEO) and executives that high-rated risk factors are managed and that appropriate controls are in place and operating effectively.[1] With increases in the regulatory regime, increasing technology complexity and pressures on cost, organisations are seeking productivity improvements in the evaluation of the performance of internal controls. One method of productivity improvement is applying technology to allow near continuous (or at least high-frequency) monitoring of control operating effectiveness, known as continuous controls monitoring (CCM).[2] CCM is a subset of continuous assurance, alongside continuous data assurance (verifying the integrity of data flowing through systems) and continuous risk monitoring and assessment (dynamically measuring risk).

Improved management and monitoring of controls through CCM (and associated risk management activities) may reduce the extent to which audit and assurance staff need to undertake annual detailed testing of controls.[3] In addition to cost reductions through improved efficiency and effectiveness (**figure 1**), other benefits include increased test coverage (through greater sampling and the ability to do more with the same or less labour), improved timeliness of testing, reduced risk velocity and potentially reduced remediation cost, greater visibility (when included in a governance, risk and compliance [GRC] solution), improved consistency, and the ability to identify trends.[4, 5] CCM also allows the replacement of manual, error-prone preventive controls with automated detective controls in which this would reduce the risk profile.[6]

The steps for implementing CCM include:[7, 8, 9]

1. Identify potential processes or controls according to industry frameworks such as COSO, COBIT® 5 and ITIL; define the scope of control assurance based on business and IT risk assessments; and establish priority controls for continuous monitoring.

Figure 1–Indicative Cost-benefit of CCM



Source: David Vohradsky. Reprinted with permission.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

Go directly to the article:

2. Identify the control objectives (or goals) and key assurance assertions for each control objective. (Guidelines for the formalisation of assertions may need to be developed as the concept of formal assertions is not well developed within IT risk).
3. Define a series of automated tests (or metrics) that will highlight (or suggest) success or failure of each assertion using a "reasonable person holistic review."[10]
4. Determine the process frequencies in order to conduct the tests at a point in time close to when the transactions or processes occur.
5. Create processes for managing the generated alarms, including communicating and investigating any failed assertions and ultimately correcting the control weakness.

DEFINING CONTROLS TO MONITOR

The scope of overall IT control assurance is usually determined from critical business and IT processes, which are prioritised based on risk and prior experience in reviewing the controls through audits, self-assessments and control breakdowns. For the purposes of example, one can assume the organisation has determined a scope of annual control assurance based on the controls in **figure 2**.

Of these controls, the priorities for implementation of CCM[11, 12, 13] should be based on risk ratings/return on investment (ROI) (such as value to the organisation) and ease of implementation (such as having readily available data from systems and controls that already have an aspect of monitoring and reporting).

Figure 2—Priority of Controls for Continuous Monitoring

In Scope Controls	System	Monitored	Metrics	Risk*	Audit ROI+
Vendor service level agreement (SLA) management	Partial	No	No?		Medium
Software development life cycle (SDLC)	No	No	Yes		Low
Human resources (HR) management	Partial	Operational	No		Medium
User access reviews	Partial	No	Partial	High	High
Segregation of duties	No	No	No		High
Change management	Yes	Operational	Yes	High	High
Incident management	Yes	Operational	Yes		Low
Backup and recovery	Yes	Operational	Yes		Low
Capacity, availability and performance	Partial	Operational	Yes		Medium
IT service continuity	Partial	No	Yes		Medium
IT perimeter security	Yes	Alerts?	No?	High	High
AV management	Yes	Alerts	Yes	Medium	High
Data loss prevention	Yes	Alerts	Yes	High	High
End point encryption	Yes	Alerts	Yes		Medium
Security monitoring	Yes	Operational	Yes	Medium	High

* Self-assessed
\+ Focus areas

Source: David Vohradsky. Reprinted with permission.

In the **figure 2** example, the high-profile controls highlighted by the internal audit function have been assessed against data availability and existing monitoring or metrics. Controls highlighted in green are candidates for continuous control monitoring (red indicates a roadblock that may preclude a control from being considered). The priority or suitability of controls for continuous monitoring also needs to consider the relationships among controls. For example, configuration and vulnerability management rely on asset management, which may be deficient and not suitable for inclusion in the scope of assurance. In such a case, the controls that depend on it may not be suitable for continuous monitoring.

IDENTIFYING ASSERTIONS

Processes for management assurance of controls are usually more informal than an audit because they are often based on professional judgment, rather than detailed testing. An audit is a systematic process in which a qualified team or person objectively obtains and evaluates evidence regarding assertions about a process and forms an opinion on the degree to which the assertion is implemented.[14] To automate an assurance process, control descriptions need to be reviewed to separate those components of the control that can be formally tested and those components that will rely on professional judgement.[15]

Internal control objectives in a business context are categorised against five assertions used in the COSO model[16]—existence/occurrence/validity, completeness, rights and obligations, valuation, and presentation and disclosure. These assertions have been expanded in the SAS 106, "Audit Evidence,"[17] and, for the purposes of a technology context, can be restated in generic terms, as shown in **figure 3**.

COSO objectives are known as enterprise goals, IT-related goals and enabler goals in COBIT 5,[18] and the financial statement assertions are loosely translated in the technology context to "completeness, accuracy, validity and restricted access."[19] Much (if not all) of the literature on CCM relates to business processes, and, as such, there is no documented alignment or mapping among IT control objectives (or goals) and the formal assertions necessary for formalised objective testing.

In an attempt to bridge this gap, **figure 4** compares example control descriptions against related guidance from an IT security context and the related COBIT 5 goals, and proposes a formal assertion that could be used in a CCM context.

DEFINING AUTOMATED TESTS

To continuously assess controls, rules need to be developed to test in real-time (or near-real-time) compliance with the

Figure 3—SAS 106 Financial Statement Assertions

Classification	Assertion
Assertions about classes of transactions and events	Occurrence: Transactions and events that have been recorded have occurred.
	Completeness: All transactions and events that should have been recorded have been recorded.
	Accuracy: Data related to the transactions and events have been recorded appropriately.
	Cut-off: Transactions and events have been recorded in the correct period.
	Classification: Transactions and events have been recorded in proper accounts.
Assertions about account balances (assets)	Existence: The assets exist.
	Rights and obligations: The entity holds or controls the rights to assets.
	Completeness: All assets that should have been recorded have been recorded.
	Valuation and allocation: Assets are included in financial statements.
Assertions about presentation and disclosure	Occurrence, rights and obligations: Disclosed transactions and events have occurred.
	Completeness: All disclosures that should have been included have been included.
	Classification and understanding: Information is appropriately presented and described, and disclosures are clearly expressed.
	Accuracy and valuation: Financial and other information are disclosed fairly and at appropriate amounts.

Source: David Vohradsky. Reprinted with permission.

Figure 4—Proposed Formal Assertions for Selected Controls			
Example Control Description	**ISO 27002 Guidance**	**COBIT 5 Process Goals**	**Proposed Formal Assertions**
All changes to the IT systems (including hardware, networks and software) are managed to minimise the likelihood of disruption, unauthorised alterations and errors.	12.5.1 (e) Obtaining formal approval for detailed proposals before work commences 12.5.1 (f) Ensuring authorized users accept changes prior to implementation 12.5.1 (i) Maintaining an audit trail of all change requests	BAI06: (a) Authorised changes are made in a timely manner and with minimal errors. (b) Impact assessments reveal the effect of the change on all affected components. (c) All emergency changes are reviewed and authorised after the change. (d) Key stakeholders are kept informed of all aspects of the change.	CM1 An authorisation has occurred prior to every change. CM2 Testing has been completed for all changes prior to implementation. CM3 An approval has occurred, indicating completeness of testing conducted. CM4 An authorisation has occurred for every emergency change.
Security measures are in place to prevent, detect and remove malicious software.	10.4.1 Installation and regular update of malicious code detection and repair software to scan computers and media as a precautionary control or on a routine basis	DSS05.01 Protect against malware. Implement and maintain preventive, detective and corrective measures in place (especially up-to-date security patches and virus control) across the enterprise to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam).	AV1 AV protection exists on all required assets. AV2 All AV signature updates that should have been made in the period have been made.
Security measures are in place to detect potential data breaches/ data exfiltration transmissions and prevent them by monitoring, detecting and blocking sensitive data.	10.8.1 (a) Procedures designed to protect exchanged information from interception, copying, modification, misrouting and destruction 10.8.1 (g) Use of cryptographic techniques	DSS05: (2) Information processed on, stored on and transmitted by end point devices is protected. (5) Electronic information is properly secured when stored, transmitted or destroyed.	DLP1 Data loss prevention (DLP) protection exists on all required assets. DLP2 End point encryption exists on all required assets. DLP3 DLP protection exists on all network paths. DLP4 DLP alerts have been accurately recorded. DLP5 All DLP alerts that should have been disclosed (and actioned) have been disclosed and actioned.
Source: David Vohradsky. Reprinted with permission.			

previously mentioned formal assertions that are required to be made about the selected controls.[20] The required tests can be classified[21, 22] into seven broad categories based on traditional audit processes or evidence types:

1. **Asset management queries** (where accurate), in place of physical examination of assets
2. **Electronic transaction confirmations**, in place of authenticated transaction documents, including verifying atomic elements of transactions
3. **Electronic statement queries**, in place of internal or external documentation
4. **Re-performance of selected controls**, using some form of automation
5. **Observation** (still a manual periodic test)
6. **Analytical procedures**, such as statistical analysis, comparisons with other internal or external data sets, and pattern-matching within transaction data
7. **Automating collation of responses** to inquiries such as control self-assessment surveys

The types of tests that could be employed in the case study example appear in **figure 5**.

Generally, tests need to answer the question: What would the data look like if the control objective was met or was not met?[23]

Asset management queries and transaction confirmation (type 1 and 2) tests can use existing or improved key risk indicators (KRIs) to provide what is described[24] as a risk indicator continuous assurance (RICA) framework. Past audit report evidence can also be used to identify sources of data and applicable analytics.[25] In this testing approach, a designated threshold being met in two or more consecutive months (or the majority of the time) may indicate a strong control, whereas the threshold not being met in two or more consecutive months may indicate a weak control.[26]

Statement (or tabular data) tests (type 3) can use a belief function approach,[27] in which evidence for and against an assertion is mathematically combined (or aggregated) to determine a result. In this approach, assurance levels are divided into five categories (very low, low, medium, high and very high) based on value ranges. For example, the strength of evidence supporting completeness of testing could be determined by ranges of test coverage or ranges of outstanding defect percentages.

Large data sets or complex behavioural controls may require analytical testing (type 6) to validate an assertion. This analysis may employ a risk score methodology[28] or probability models[29] to create an equal distribution of values 0 to 1 across all samples, with bands reflecting confidence in the assertion. The analysis may be based on:

- Higher or lower than expected values
- Expected or opposite to expected movement
- Small or large changes from one period to the next
- Process metrics
- Erratic behaviour or volatility (variance) in the process

Figure 5—Assertion Test Plan

Proposed Assertion (Refer to figure 4)	**Test Type** (Refer to seven test types noted previously)	**Proposed Pass Condition for Test to Indicate a Strong Control**
CM1. An authorisation has occurred for every change.	(2) Transaction confirmation	Percentage of changes with prior authorisation meeting the threshold for last two consecutive months
CM2. Testing has been completed for all changes prior to implementation.	(3) Statement (test results) query (6) Analytical procedure	High or very high confidence in testing for last two consecutive months, based on number of open defects
CM3. An approval has occurred for completeness of testing conducted.	(2) Transaction confirmation	Percentage of changes with testing approvals meeting threshold for last two consecutive months
CM4. An authorisation has occurred for every emergency change.	(2) Transaction confirmation	Percentage of emergency changes with authorisation meeting threshold for last two consecutive months
AV1. AV protection exists on all required assets.	(1) Asset management query	Percentage of required assets with AV protection meeting threshold for last two consecutive months
AV2. All AV signature updates that should have been made in the period have been made.	(2) Transaction confirmation	Percentage of assets with the latest AV signature meeting threshold for last two consecutive months
DLP1. DLP protection exists on all required assets.	(1) Asset management query	Percentage of required assets with DLP protection meeting threshold for last two consecutive months
DLP2. End point encryption exists on all required assets.	(1) Asset management query	Percentage of required assets with end point encryption meeting threshold for last two consecutive months
DLP3. DLP protection exists on all network paths.	(4) Re-performance (with test data) (7) Vendor control self-assessment	Result of weekly automated control tests to trigger DLP events, passing on two consecutive months (36 per annum)
DLP4. DLP alerts have been accurately recorded.	(4) Re-performance (with test data) (6) Analytical procedure	Result of weekly automated control tests to trigger DLP events, passing on two consecutive months (36 per annum)
DLP5. All DLP alerts that should have been disclosed (and actioned) have been disclosed and actioned.	(6) Analytical procedure	Statistical analysis of DLP alerts and corresponding incident actions to determine volatility of process

Source: David Vohradsky. Reprinted with permission.

Assertions that need to be tested by subjective judgement (type 7, such as those obtained through control self-assessments by service managers or vendors) can be validated[30] through the Delphi Method. In this approach, a more accurate consensus of control effectiveness is obtained through one or more rounds of anonymous self-assessments, which may be reviewed, and feedback provided by experts between rounds.

Planning for the implementation of any of the previously described automated tests needs to take into account likely difficulties such as obtaining data management approvals; data sourcing and aggregation lead times; the need for control domain expertise; technology acquisition and integration costs; and the need for information sharing and coordination among audit, risk and compliance functions.[31]

REPORTING

Figure 6 shows the governance and management processes associated with control assurance. Management monitors processes through mechanisms including KRIs, which are used to alert the business to potential control issues and are part of a continuous improvement cycle.

CCM takes selected KRIs and the results of other tests and analytics on processes and forms part of an overall control assurance program (CAP) in which the concerns over the monitored controls are validated before being prioritised and acted upon alongside issues identified by other periodic manual testing.[32] Additional risk and key control deficiencies may also be identified through management risk and control self-assessments (RCSA) that form part of the program based on management knowledge gained through operating the plan-build-run-monitor cycle. Integrated issue management using a GRC platform facilitates[33] digitisation, automation of alerts and management of remediation activities, once agreed upon by management.

Mature KRIs linked to formal assertions are continuously monitored and reported, automatically form part of the risk and control profile, and are integrated into daily management processes.[34]

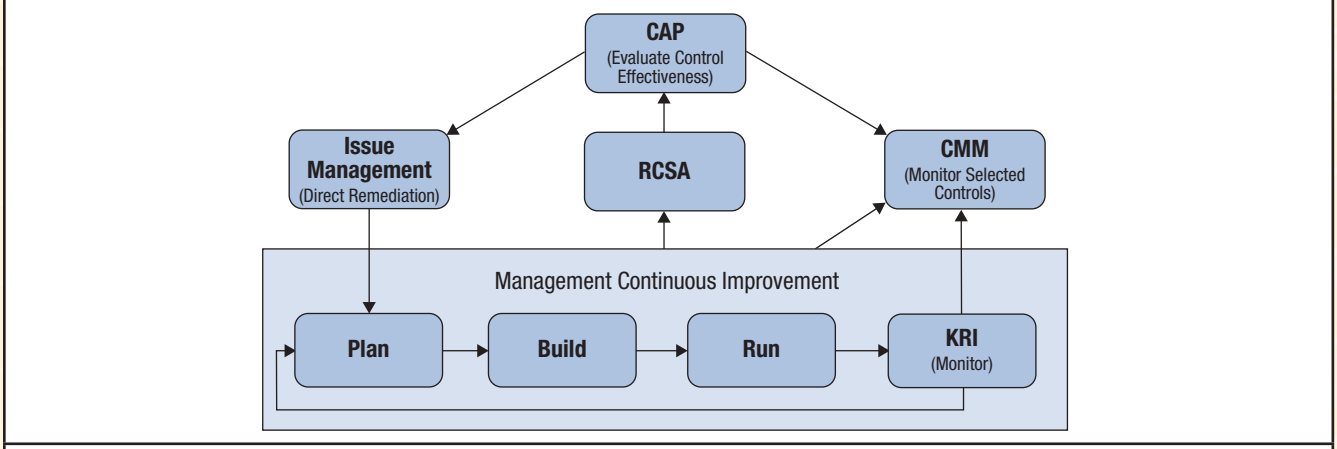
Other KRIs that may be subject to false positives are used in day-to-day management of the process in question and adjusted to a point where they can be relied upon for management self-assessment and continuous improvement of the process.[35] As they mature, they can be incorporated in an expanded CCM regime.

CONCLUSION

This article provides guidance on the identification and prioritisation of controls for CCM implementation and introduces the need to transform COBIT® (and other) management practices into formal assertions (in line with SAS 106) in order to facilitate objective automated testing. It defines the categories of testing available, maps a sample set of assertions to testing types and provides high-level guidance on applicable test rules.

Further work is needed to define formal assertions for the complete set of COBIT 5 management practices as a necessary

Figure 6—Control Assurance Processes



Source: David Vohradsky. Reprinted with permission.

precursor to the wider use of CCM within an IT risk context. This work ideally should occur with further development of *COBIT® 5 for Risk* and other COBIT guidance from ISACA®.

ENDNOTES

[1] Coderre, D., *Global Technology Audit Guide—Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment*, Institute of Internal Auditors, 2005

[2] Vasarhelyi, M. A.; M. Alles; K. T. Williams; 'Continuous Assurance for the Now Economy', Institute of Chartered Accountants in Australia, 2010

[3] MarFan, K.; IT Audit and Assurance Guideline G42, Continuous Assurance, ISACA, 2010, *www.isaca.org/standards*

[4] Deloitte, *Continuous Monitoring and Continuous Auditing: From Idea to Implementation*, 2010

[5] Gohil, J.; 'Reduce Audit Time Using Automation, by Example', presentation to ISACA Atlanta Chapter, Protiviti, 2013

[6] *Op cit*, Deloitte

[7] *Op cit*, Coderre

[8] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC27002:2006, *Information Technology—Security techniques—Code of practice for information security management*, 2006

[9] *Op cit*, Vasarhelyi 2010

[10] *Op cit*, Standards Australia

[11] *Op cit*, Deloitte

[12] *Op cit*, MarFan

[13] *Op cit*, Vasarhelyi 2010

[14] ISACA, *2009 CISA Review Manual*, USA, 2008

[15] *Op cit*, Vasarhelyi 2010

[16] ISACA, *Relating the COSO Internal Control—Integrated Framework and COBIT*, USA, 2014

[17] American Institute of Certified Public Accountants (AICPA), SAS 106, 'Audit Evidence', February 2006

[18] *Op cit*, ISACA 2014

[19] ISACA, *IT Assurance Guide: Using COBIT*, USA, 2007

[20] *Op cit*, Coderre

[21] Majdalawieh, M.; S. Sahraoui; R. Barkhi; 'Intra/Inter Process Continuous Auditing (IIPCA), Integrating CA Within an Enterprise System Environment', *Business Process Management Journal*, 18 (2), 2012, p. 304-327

[22] Vasarhelyi, M. A.; M. G. Alles; A. Kogan; 'Principles of Analytic Monitoring for Continuous Assurance', *Journal of Emerging Technologies in Accounting*, vol. 1, p. 1-21, 2004

[23] *Op cit*, Coderre

[24] Nigrini, M. J.; A. J. Johnson; 'Using Key Performance Indicators and Risk Measures in Continuous Monitoring', *Journal of Emerging Technologies in Accounting*, vol. 5, 2008, p. 65-80

[25] *Op cit*, Vasarhelyi 2010

[26] *Op cit*, Dale

[27] Mock, T.J.; A. Wright; R. P. Srivastava; 'Audit Program Planning Using a Belief Function Framework', Proceedings of the 1998 Deloitte & Touch University of Kansas Symposium on Auditing Problems, USA, 1998, p. 115-142

[28] *Op cit*, Nigrini

[29] Alles, M. G.; A. Kogan; M. A. Vasarhelyi; 'Putting Continuous Auditing Theory Into Practice: Lessons From Two Pilot Implementations', *Journal of Information Systems*, 22 (2), 2008, p. 195-214

[30] *Op cit*, Vasarhelyi 2010

[31] Vasarhelyi, M. A.; S. Romero; S. Kuenkaikaew; 'Adopting Continuous Auditing/Continuous Monitoring in Internal Audit', *ISACA Journal*, vol. 3 , 2012, p. 1-5

[32] *Op cit*, Coderre

[33] Schermann, M.; M. Wiesche; H. Krcmar; 'The Role of Information Systems in Supporting Exploitative and Exploratory Management Control Activities', *Journal of Management Accounting Research*, vol. 24, 2012, p. 31-59

[34] Dale, J.; E. Chung Yee Wong; 'Achieving Continuous IT Auditing: RICA', *ISACA Journal*, vol. 6, 2009, p. 1-5

[35] *Op cit*, Coderre