Defining Targets for Continuous IT Auditing Using COBIT 2019

I have previously discussed sitting and passing my Certified Information Systems Auditor® (CISA®) exam back in 2005.1 I tend to remember that one of the hot topics at that time was continuous online auditing. The approach allowed IT auditors to monitor system reliability on a continuous basis and to gather selective audit evidence through the computer.2 However, the focus then was very much on auditing the transactional data from applications. One of the key perceived benefits was the change from periodic reviews of a sample of transactions to ongoing audit testing of 100 percent of transactions.3

Although some practitioners had adopted continuous auditing for IT audit purposes,4 it took the second edition of the Institute of Internal Auditor’s Global Technology Audit Guide (GTAG) 3: Continuous Auditing: Coordinating Continuous Auditing and Monitoring to Provide Continuous Assurance, 2nd Edition to popularize a focus expansion to include not only transactional data, but also other data sources such as security levels, logging, incidents, unstructured data, and changes to IT configurations, application controls, and segregation of duty (SoD) controls.6 So what is continuous auditing and how can it be used by auditors to audit IT processes?

Defining Continuous Auditing

Continuous auditing is not the same as continuous monitoring. There may very well be instances (e.g., in different enterprises) where both are performing the same function and utilizing the same underlying code, but the key difference is the owner of the process. Continuous monitoring is a management process that monitors whether internal controls are operating effectively on an ongoing basis.7 In other words, it is performed by the first or second line. Continuous auditing is performed by audit and is designed to enable the internal auditor to report on subject matter within a much shorter time frame than under the traditional retrospective approach (figure 1).8

Continuous auditing is achieved through ongoing risk and control assessments enabled by technology-based audit techniques such as generalized audit software, spreadsheet software or scripts developed using audit-specific software, specialized audit utilities, computer-aided audit tools (CAATs), commercially packaged solutions and custom-developed production systems.9 In short, continuous auditing is about using technology to measure and report on risk indicators.
Identifying Risk Indicators

A risk indicator is a metric capable of showing that the enterprise is subject to, or has a high probability of being subject to, a risk that exceeds the defined risk appetite. Identification of quality risk indicators is, therefore, critical to performing continuous auditing over IT processes.

In COBIT®, a management objective always relates to one process (with an identical or similar name) and a series of related components of other types to help achieve the objective. These processes are, in turn, broken down into management practices, each of which has defined sample metrics (figures 2, 3 and 4).

I am proposing that many of these metrics can be used as risk indicators for continuous IT auditing purposes. The key to identifying the useful metrics is to ascertain whether there are two or more sources of information that can be clashed to produce reliable figures.

For our first example, to measure the number of emergency changes not authorized after the incident, this might involve, for instance, clashing the data from a release management application with the data from a change management application. Having a common identifier between these applications is key.

For our second example, to measure the average downtime per critical asset, clashing the data from the asset register with the data from an incident management system would produce the desired result, most likely matching the asset ID.

For our third example, to measure the average time between change and update of accounts might involve, for instance, clashing the data from a service desk application with data from, say, the

![Figure 2—Sample COBIT Management Practice 1](source: ISACA, COBIT® 2019 Framework: Governance and Management Objectives, USA, 2018)

<table>
<thead>
<tr>
<th>Management Practice</th>
<th>Example Information Security-Specific Metrics</th>
</tr>
</thead>
</table>
| **BAI06.02 Manage emergency changes.** | a. Number of emergency changes not authorized after the incident  
b. Percent of total changes that are emergency fixes |
| Carefully manage emergency changes to minimize further incidents.  
Ensure the emergency change is controlled and takes place securely.  
Verify that emergency changes are appropriately assessed and authorized after the change. | |

![Figure 3—Sample COBIT Management Practice 2](source: ISACA, COBIT® 2019 Framework: Governance and Management Objectives, USA, 2018)

<table>
<thead>
<tr>
<th>Management Practice</th>
<th>Example Information Security-Specific Metrics</th>
</tr>
</thead>
</table>
| **BAI09.02 Manage critical assets.** | a. Number of critical assets  
b. Average downtime per critical asset  
c. Number of incident trends identified |
| Identify assets that are critical in providing service capability. Maximize their reliability and availability to support business needs. | |

![Figure 4—Sample COBIT Management Practice 3](source: ISACA, COBIT® 2019 Framework: Governance and Management Objectives, USA, 2018)

<table>
<thead>
<tr>
<th>Management Practice</th>
<th>Example Information Security-Specific Metrics</th>
</tr>
</thead>
</table>
| **DSS05.04 Manage user identity and logical access.** | a. Average time between change and update of accounts  
b. Number of accounts (vs. number of authorized users/staff)  
c. Number of incidents relating to unauthorized access to information |
| Ensure that all users have information access rights in accordance with business requirements. Coordinate with business units that manage their own access rights within business processes. | |
Microsoft Active Directory (AD). Again, having a common identifier, likely the user ID, is key.

Further, many of the COBIT-defined metrics may be key risk indicators (KRIs), a subset of risk indicators that are highly relevant and possess a high probability of predicting or indicating important risk12 or, where risk is not measured, key performance indicators (KPIs), a measure that determines how well the process is performing in enabling the goal to be reached in the enterprise under review. These will also add value to any continuous audit program.

In addition, ongoing control assessments need not run in real time. The frequency of analysis should be determined by the level of risk, the business process cycle and the degree to which management is monitoring the controls.13

Improving the Control Environment

When a continuous auditing program is working well for a period of time, it may be possible to transfer the workload from audit to management. In this case, continuous auditing becomes continuous monitoring. Audit will now provide continuous assurance, a combination of continuous auditing and testing of first and second lines of defense continuous monitoring (figure 5).14 In this manner, audit can focus on new metrics, which, in turn, can be transferred to management, continuously improving the control environment.

Conclusion

Audit is always under pressure to prove its value to the business. This can be achieved in the first instance by identifying, measuring and reporting upon risk indicators. Further value can be added by transferring these newly defined controls to the first and second lines while developing new metrics. Finally, where these risk indicators relate to management practices and, in turn, management objectives, an audit’s value can be demonstrated clearly.

Endnotes

2 ISACA®, CISA Review Manual 2005, USA, 2004
3 The Institute of Internal Auditors (IIA), Global Technology Audit Guide (GTAG) 3, Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment, USA, 2005
7 Ibid.
8 Ibid.
9 Ibid.
12 ISACA Glossary, “Key Risk Indicator,” https://www.isaca.org/resources/glossary
13 Op cit IIA, 2015
14 Ibid.