Audit-focused Mining—New Views on Integrating Process Mining and Internal Control

Most approaches to process audits are antiquated and far from best utilizing the auditor’s capabilities or the potential of existing enterprise resource planning (ERP) data. Instead, it would be ideal to start a process audit fieldwork project with the best information set available: complete models of actual processes conveniently displayed even on mobile devices, data analytics finished with high-risk business transactions clearly indicated, internal controls evaluated to the maximum extent and all results directly linked to the auditee’s financial statements.

To systematically build a better approach to process auditing in an ERP environment, it is important to understand the way process audits are carried out at present. A closer look at current audit practice reveals two major shortcomings:

1. For complex audit assignments such as process audits, primarily manual audit procedures are employed. The manual survey of as-is processes by interviews/inquiries or sample-based inspections of control evidence documentation are common examples. This circumstance is particularly surprising in light of the fact that almost all audit-relevant data are available in the entity’s IT environment. For audit purposes, IT tools are preponderantly used for single audit steps. For instance, IT-based data analyses are applied for substantive testing to identify conspicuous business transactions (e.g., SAS 99). However, in current practice, a comprehensive view on IT support is seldom taken, especially not for complex audit tasks like process audits.

2. Although business processes and IT are highly intertwined on the client side, auditors typically do not use an integrated audit approach. Processes and IT are audited separately by different auditors who are organized in different departments. Results are integrated but not before the reporting step of the assignment. All this happens even though an integrated approach for process and IT audit has been proven to be more efficient (saves time) and effective (a more comprehensive audit plan, more likely to identify risk exposures).

What deters auditors from overcoming these shortcomings with the help of IT? How is an IT-based, data-driven and integrated audit procedure composed to make the difference?

DATA-DRIVEN APPROACH TO PROCESS UNDERSTANDING

In the course of a process audit (Figure 1), an auditor essentially has to answer four questions:

1. Which process (variants) does he/she have to audit (scoping)?
2. In which variants was the process enacted during the period under audit (walk-through)?
3. Which control means were effectively in place (internal controls [IC] testing)?
4. What is the overall audit result for the process (reporting)?

Phase 2, the walk-through, is the first potential area for automation. The domain of process mining provides a set of techniques to discover real processes by extracting knowledge from recordings of past process executions (e.g., SAS 99). However, in current practice, a comprehensive view on IT support is seldom taken, especially not for complex audit tasks like process audits.

2. Although business processes and IT are highly intertwined on the client side, auditors typically do not use an integrated audit approach. Processes and IT are audited separately by different auditors who are organized in different departments. Results are integrated but not before the reporting step of the assignment. All this happens even though an integrated approach for process and IT audit has been proven to be more efficient (saves time) and effective (a more comprehensive audit plan, more likely to identify risk exposures).

What deters auditors from overcoming these shortcomings with the help of IT? How is an IT-based, data-driven and integrated audit procedure composed to make the difference?

**Figure 1—Process Audit Phases**

<table>
<thead>
<tr>
<th>Scoping</th>
<th>Walk-through</th>
<th>IC Testing</th>
<th>Reporting</th>
</tr>
</thead>
</table>

©2014 ISACA. All rights reserved. www.isaca.org
to human error and based on data that are independently recorded from the auditee.5, 6

However, using traditional process mining techniques in ERP environments is still a challenge. Common ERP systems (e.g., SAP, Oracle, Microsoft) are not process-oriented.7 Data that relate to particular steps of a process execution are spread across several database tables without readily providing a process-oriented link (case identifier). Hence, process mining on ERP data demands comprehensive preprocessing.

Against this background, financial process mining (FPM) was developed. It uses links between financial documents to reconstruct single-process instances.8 These links stem from fundamental accounting principles (e.g., open-item accounting) and, therefore, are available in diverse types of ERP systems. With this, all documents belonging to a particular business transaction can be automatically identified. In this regard, a business transaction—for instance, the purchase of a specific raw material—comprises several documents, from a purchase order over the goods receipt and the invoice to the payment of the vendor. These documents can be easily mapped to well-defined activities in the purchase-to-pay (P2P) process.

Based on the full set of process instances executed throughout the period under audit, a complete process model is derived by applying common process-mining techniques. Such a process model helps to get a general understanding of what has actually happened in the auditee’s business processes. Attaching the frequency of occurrence to activities enables a convenient identification of standard process flows as well as outliers. Furthermore, a drill-down to single-process instances allows for a detailed analysis of conspicuous business transactions. Figure 2 provides an example of a process model and a corresponding process instance for the P2P cycle. The process model is derived with the process-mining software Disco.9

The financial-document-based mining of business processes provides another advantage for auditors. The financial perspective of a process is readily available on the process model and process instance levels. This allows for a detailed analysis of the impact each process activity, each process instance and, in aggregation, each process has on specific financial accounts. The right portion of figure 2 includes this financial perspective in the style of t-accounts, with which auditors and accountants are familiar.10 Such detailed information on the financial impact of processes enables a new way of materiality-based scoping. So far, auditors have been mostly forced to apply a “rule of thumb” when deciding which process variants to audit for particular accounts. For instance, in a case in which the liability accounts are identified as material, the P2P cycle is usually audited. However, it is not immediately apparent for the auditor which process variants exist for the P2P cycle and to what extent each variant contributes to the balance of the material accounts. With FPM, a process model can be derived that is based only on process instances touching the in-scope accounts above a specified amount. Until now, such a deep connection between financial statements and business processes was not available for auditors.11

**AUTOMATICALLY EVALUATING INTERNAL CONTROLS**

As a result, FPM establishes a detailed and pinpointed basis for process analysis, namely the end-to-end process instance, including a direct link to the financial statements. Based on such detailed information, several internal-control-related aspects can be reviewed immediately at the process and instance levels. The analysis of the process structure reveals conspicuous, unexpected or noncompliant business transactions. Deviations from a defined standard process or applicable regulatory requirements, as well as missing process activities (e.g., approval steps for each purchase order and/or invoice), incorrect ordering of activities (e.g., payment before an invoice is received) and segregation-of-duty conflicts can be easily identified. For instance, in the left portion of figure 2, it is apparent that 42 goods receipts were posted without a corresponding purchase order. This should not be the case in a well-organized purchasing process. This kind of analysis can be performed either manually or automatically by applying conformance- and rule-based checking techniques.12, 13 In the aggregate, the auditor obtains a clear overview of what has actually happened in the process under audit.

Over and above this, current ERP systems and accounting information systems (AIS) offer a wide range of audit-relevant customizing settings, collectively referred to as application controls (ACs).14 Common examples for this type of control means are checks for duplicate invoices, the reconciliation of totals after processing a batch of payments or restricting/separating access to sensitive system functions.15, 16 ACs can be audited by directly reviewing the corresponding
customizing settings in the system. However, this review requires an in-depth knowledge of the particular ERP system and may involve a set of interlinked settings for a single AC. Hence, this review is often done by IT auditors and not by process auditors. As the corresponding settings are electronically stored in the systems, they can also be analyzed automatically. In academia, a few software solutions are discussed that operate independently from a particular ERP system and enable such an automated evaluation of ACs from an audit perspective.\textsuperscript{17, 18} As result, these solutions provide a report that includes the current settings of relevant ACs; a description of the ACs; a risk estimation based on default values; and, in case of deviations, recommendations for improvement. Thereby, these solutions hide the technical details from the auditor. Figure 3 depicts such an automatically generated report on three ACs from a SAP ERP.

In addition to the current settings, ERP systems maintain a log of changes to relevant settings including the change date, old value and new value of the parameter. The analysis of this log allows reconstructing the AC settings for each point in time throughout the audit period.

**INTEGRATING RESULTS OF IT AND PROCESS AUDIT**

A good approach to leveraging the previous results (process model/process instances and internal controls analysis) is the seamless integration of process instances and process-dependent internal controls. The integrated business process model forms the focal point of a process audit. The automated approach for integration is based on the relationship between ACs and particular process activities in the form of functional modules in the ERP system (e.g., transaction codes in SAP ERP).\textsuperscript{19, 20} For instance, a check for duplicate invoices is performed before or after process activities that involve invoice processing.
Figure 4 depicts the process model from figure 2 enriched with information on two ACs (double invoice check and payment block removal). Depending on the list of related process activities-functional modules, the nature of the control (preventive, detective) and the status of the AC settings (active, inactive), the ACs are added as a special process activity. In doing so, the structure of an enriched process model shows whether ACs were appropriately activated throughout the period under audit. For instance, in figure 4, there are business transactions for which the invoices were not checked for duplicates (all invoices that were created with the functional module MR01—Process Incoming Invoice). A drill-down displays the corresponding business transactions for a more detailed review. In contrast, for the remaining invoices (FB60—Enter Incoming Invoices) duplicates are prevented by an AC. In addition, for all invoices, the removal of a payment block during payment processing is prevented. In general, with the approach described previously, ACs as well as manual control means can be added to process instances or models.

Accordingly, with the enhanced process model, new process variants are derived enabling the auditor to better analyze process variants according to their risk and control scheme. The auditor is able to focus on business transactions that are less controlled and, therefore, are subject to a higher risk of (un)intended errors.

Again, these analyses on internal controls can be performed either manually or automatically by applying conformance- and rule-based checking techniques. Unmitigated risk, unaddressed control objectives or missing control means are available at the click of a button.
SUBSTANTIALLY AUDIT ONLY THE INTERESTING STUFF
Automated analyses on multiple aggregation levels (process activity, process instance, process model, financial account) help to focus on the most relevant audit issues. Integrating various perspectives helps to draw a complete picture. To do so:
• Identify unusual process sequences in a process model.
• Analyze conformance to standard processes and compliance requirements.
• Detect insufficiently controlled process variants and process instances.
• Pinpoint actual segregation-of-duty conflicts on the process instance level.
• Filter on particular material financial accounts, divisions or departments.

Based on these individual indicators, an overall risk score can be computed for each process instance—and in aggregation for each process variant and even in total for a financial account or an arbitrary list of accounts. A drill-down back and forth allows for diving into details or setting a particular finding in its broader context. Compared to traditional solely document-based data analyses, such an integrated view drastically reduces the number of false-positives.

USE CASE EXAMPLE
At present, the described approach for IT-based process audits is implemented at the University of Hamburg (Germany) as a software prototype called App2Audit. Figure 5 gives a rough impression of the targeted user interface.

The aim of the prototype is to show that for complex audit assignments, a comprehensive software support is feasible and auditors benefit from an integrated view on diverse data analyses.
CONCLUSION
As demonstrated, comprehensive IT support gives auditors the opportunity to better utilize their time for value-added and high-risk tasks.21, 22 In light of the increasing complexity of auditees’ business processes and the vast amount of audit-relevant data, it is crucial to be able to render audit assignments in an effective and efficient way. Of course, human auditors cannot completely be replaced by automated approaches, thus final audit assessments should undergo a professional judgment. However, in current audit practice there is significant room for improvement for an extended usage of IT support in the preparation phase of an audit. Auditors can leverage different IT-based analysis opportunities. As a result, such a comprehensive usage of IT may completely change the way audits are executed.

ENDNOTES
3 Ibid.
6 Omoteso, K.; Audit Effectiveness: Meeting the IT Challenge, Gower, UK, 2013
7 Van der Aalst, W. M. P.; K. M. van Hee; J. M. van Werf; M. Verdonk; “Auditing 2.0: Using Process Mining to Support Tomorrow’s Auditor,” Computer, vol. 43, 2010, p. 90-93
15 Bellino, C.; J. Wells; S. Hunt; Global Technology Audit Guide (GTAG) 8: Auditing Application Controls, 2007
21 Op cit, Omoteso