CHAPTER 20

WHAT TO LOOK FOR IN AUDIT OPERATIONS APPLICATIONS

Julia Koo

The highest priority of any company's executive is to increase shareholder value. Moreover, Sarbanes-Oxley (SOX) has put something further on executives' minds: criminal liability. This chapter tells how an audit operations application addresses both of these issues. Furthermore, it discusses what considerations there are for choosing the one application that suits your needs—for both today and tomorrow; it analyzes today's pain points, presents current basic and advanced feature requirements for these audit operations applications, and foresees next generation applications' architecture.

20.1 AUDIT PROCESS

Audit is not a new concept to companies. The internal audit department's and external auditors' involvement in ensuring financial reporting accuracy has always been a part of doing business. Exhibit 20.1 shows an example of a simple internal audit process. Companies may have different versions of this process.

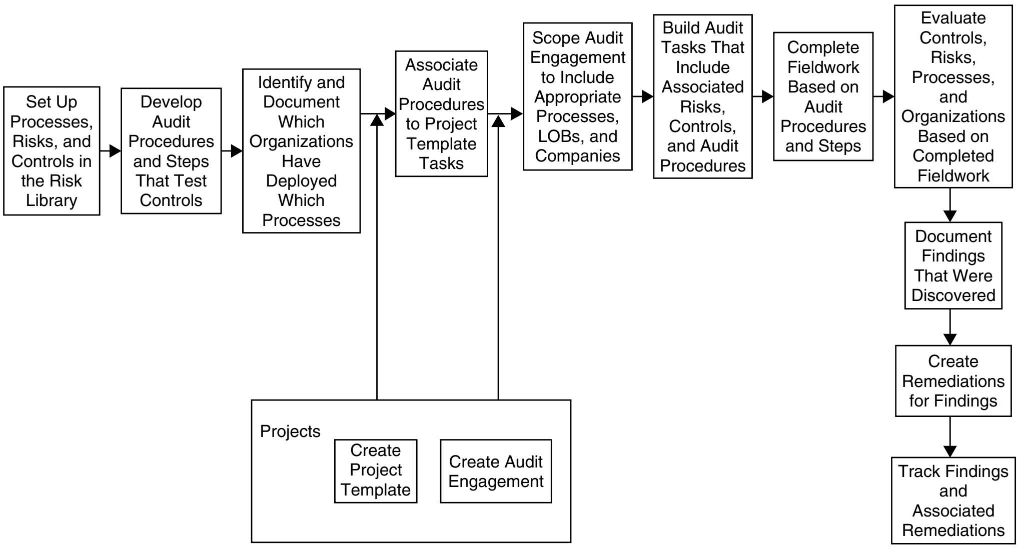

Set Up Processes, Risks, and Controls in the Risk Library
Develop Audit Procedures and Steps That Test Controls
Identify and Document Which Organizations Have Deployed Which Processes
Associate Audit Procedures to Project Template Tasks
Scope Audit Engagement to Include Appropriate Processes, LOBs, and Companies
Build Audit Tasks That Include Associated Risks, Controls, and Audit Procedures
Complete Fieldwork Based on Audit Procedures and Steps
Evaluate Controls, Risks, Processes, and Organizations Based on Completed Fieldwork
Document Findings That Were Discovered
Create Remediations for Findings
Track Findings and Associated Remediations
Projects
Create Project Template
Create Audit Engagement

EXHIBIT 20.1 INTERNAL AUDIT PROCESS

Starting from the basic setup in *risk library* as a centralized repository to allow data reuse, companies need to work with different constituents from different lines of business to draft and finalize business processes definitions, risks associated with each process and subprocess, and controls established to mitigate these risks. These processes, risks, and controls usually have a many-to-many relationship; hence any changes made to these objects and relationships should be tracked and should allow all involved parties to see the changes made and approve accordingly. After controls are identified and put in place to mitigate risks, companies need to ensure periodically these controls are working properly. This is usually done by the independent internal audit department to ensure neutrality. In order for internal auditors to carry out tests, audit procedures and testing steps have to be predefined collaboratively between business process owners and internal audit.

For companies with multiple organizations, especially internationally corporations, processes could vary in definition from one organization to another. This could be due to different national laws or adaptation to local business practices. Regardless of these factors, companies need to instantiate processes in organizations and make definition changes accordingly to reflect the true nature of each organization's operational process. Some organizations don't even deploy all processes. Therefore, instantiation of processes at organization level is essential in representing operations correctly for audit purposes.

To ensure controls effectiveness, companies need to do periodic testing and auditing. The general practice is to have the audit project set up and scoped to perform testing on certain areas, such as in a particular organization, for a certain business process, or for any particular regulation. Because these audit projects could be performed periodically, it is a general practice for companies to have created audit project templates that include all the necessary work papers. So when a project is needed, all the auditors need to do is to pull out the template and create a new project based on the template. The template could include the scope of testing, tasks to be performed, predefined spreadsheets as work papers, and any supporting documents.

At the testing time, auditors perform the testing steps and record their evaluation opinions. These opinions need to have bases, so storing supporting evidence and linking them correctly to each opinion is essential for future reference. During testing, auditors are likely to discover trouble areas and places that need to be improved. These concerns should then be documented, assigned, and tracked. A full audit trail is needed to prove that weaknesses, especially material ones, have been discovered, investigated, and mitigated. For this purpose, companies usually use findings or issues to document problems exposed during auditing.

Throughout the audit process, the audit department might have recommendations for improving said process. These improvements can then be proposed to the audit executives, CFO, audit committee, and other constituents for approval. This is a feedback loop into the audit process to improve its efficiency and reliability.

20.2 AUDIT OPERATIONS MATURITY MODEL

A maturity model is usually used by companies to analyze process efficiency. Different versions of this maturity model could be used to analyze the effectiveness of an audit process. The movement from the bottom left corner to the top right corner in Exhibit 20.2 indicates improvement in efficiency of the measured process. The following is one of the possible illustrations of how a maturity model could be used to analyze the audit operations process.

There are five levels in a standard maturity model: *Initial*, *Repeatable*, *Defined*, *Managed*, and *Optimizing*. Level 1 is the initial level where companies are using manual processes to manage disparate information around auditing. Printouts of spreadsheets and documents have to be stored securely in a filing cabinet under a certain order for recovery purposes. For the scope of this discussion, level 2 (*Repeatable*) and level 3 (*Defined*) have been consolidated into one level. At level 2, the process should have been documented but not standardized throughout the enterprise, whereas at level 3, the process has been documented and standardized. For compliance purpose, companies usually achieve level 2 and level 3 together. While they are documenting their processes thoroughly, they also try to standardize them across the enterprise and document any variations that might have been encountered at certain organizations. Hence, level 2 and level 3 are condensed into one level: *Defined*. At this level, audit operations application,

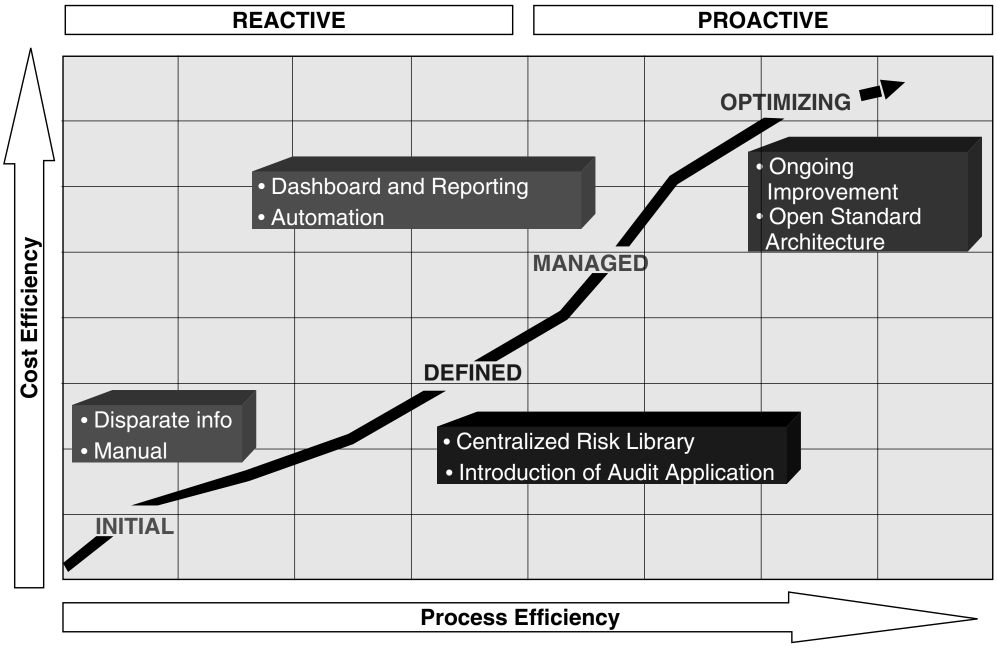


EXHIBIT 20.2 INTERNAL AUDIT OPERATIONS MATURITY MODEL

along with its infrastructure, needs to be introduced to have a centralized repository of processes, risks, and controls and associations among them. At level 4 (*Managed*), performance measures are put in place to measure success. Control automation is also introduced on this level to help in improving testing efficiency and reliability. The final level is the *Optimizing* level. At this level, the audit process is being watched constantly for continuous improvement. It is being tied to the broader corporate performance management, integrated into daily business operations, and infused as part of the open standardized IT infrastructure.

In the following section, this maturity model will be used to analyze the audit operations process in greater detail. It will be shown what companies need from different applications at each level, and what to expect in the future if a movement from one level to another is desired. However, since companies could be very different in nature (e.g., industry, geographical area, budget allocation, etc.), it is up to each individual company to estimate which level it currently is at and which level it would like to be at in the future; then it can plan its budget, resource allocation, and application purchases accordingly.

20.3 BUSINESS PAIN POINTS (LEVEL 1: INITIAL)

Most, if not all, accelerated filers of the Sarbanes-Oxley Act (SOX) have moved away from this level because the law requires them to document their processes, put controls in place to mitigate risks, track findings and issues, and report on issues and bad business conducts that might have surfaced. It is hard for companies to remain on this level with these SOX requirements. At this level, companies are using manual processes to track audit-related information, including project scoping, testing, evidence tracking, trouble logging, and data reporting. Electronic and physical documents, spreadsheets, and manually consolidated reports are usually the vehicles of the process. Information sharing depends on individuals' gratitude. Reliability of data depends on people's integrity. There is usually a lack of security, access control, and status tracking at this level.

20.4 VALUE PROPOSITION OF AUDIT OPERATIONS APPLICATIONS

There are several reasons why companies should move from the initial level to the other levels:

- Cost reduction
- Reliability enhancement
- Visibility improvement

(a) COST REDUCTION. Audit operations applications should provide a centralized risk library that can be leveraged across all departments and locations. The audit application can also act as the single source of truth of all testing results. This single repository simplifies training for new auditors, increases productivity of existing ones, and allows information sharing with external auditors to become a "click of a button" activity to generate auditor-ready reports on testing results and findings. Furthermore, if a control is information technology (IT) focused or system orientated, testing scripts can be set up in the audit application to generate automated testing results, link those results to a control, state an appropriate control testing opinion, and prompt auditors for opinion review. In addition, this whole process could be repeated at any interval of time at an auditor's preference. This transforms manual testing by auditors into automated control testing by the application. Auditors will only need to review these results. The increased productivity, simplified training, and reduced testing scope for internal auditors will help companies to cut costs.

On top of internal cost saving, external cost saving is also very significant. Companies spent $1 million to $8 million in year 1 of SOX.[1] Most of the expenditures went to external auditors for their time spent in gathering evidence on controls. An audit application allows companies to share internal audit testing results and evidence with external auditors quickly and easily through auditor-ready reports. These reports tend to be in PDF format, which cannot be edited; hence it is trusted by external auditors. With information sharing being simplified, it usually implies smaller test scope by the external auditors before their attestation to control efficiency of the company. With automated controls, the testing time by external auditors will be reduced, even if these controls remain in scope for external auditors. All of this time reduction translates into cost savings for companies.

One advanced feature (a complete features list will be presented later) of audit applications is transaction abnormality alerts. This kind of alert is referred to as proactive controls. It is apparent that if a problem is dealt with earlier, the loss could be managed better and the cost of loss should be lower. Proactive control allows you to do exactly that. Potential problems are sometimes predictable earlier in time through transaction observation. However, manual transaction monitoring or sampling could be costly and error prone. Hence, audit applications provide the capability of rule engines, validation alerts, and trend tracking. With these capabilities, companies can deal with a problem earlier in time, sometimes even before the problem occurs. Change of a policy, investigation of an employee, and discontinuing a supplier contract are all possible resolutions of potential problems, such as fraudulent events and unreliable suppliers.

In short, with audit operations applications, cost reduction can be realized from increased productivity of internal staffs, lower external auditor costs, and transaction abnormality alerts that prompt immediate attention and actions.

(b) RELIABILITY ENHANCEMENT. Automated controls not only reduce costs, but also increase reliability because results come directly from the companies' operational IT system. By eliminating human involvement in control testing, risk of error and fraudulent events can be considered as nonexistent in this type of control.

Audit applications should inherently consist of a work flow engine that mandates the audit process's flow. Areas such as approval and task dependency should be enforced by the work flow engine. For instance, without proper review, high-impact issues cannot be closed. This kind of enforcement can ensure that a standard policy is followed; hence it increases reliability in the data being reported for compliance purposes.

(c) VISIBILITY IMPROVEMENT. With disparate information, reporting is meaningless because data cannot be guaranteed to represent a holistic view of the business. Furthermore, meaningful conclusions can be difficult to reach when using data comparison without a common reference. For example, an issue resolution cycle time in the sales department is 30 days on average, whereas the same measure of the service department is 5 days on average. By looking at this comparison, one might conclude that the sales department needs to improve its issue resolution time. However, a further investigation into the data might be able to paint a more complete picture that the sales department already has good controls in place and all issues are minor ones, whereas the service department is still installing proper controls, so issues are major and have taken a majority of time of managerial resources in that department; hence service performance for the past month had been compromised.

This simple example illustrates how important it is to do analysis in combination with data from different business areas. Reporting solely on audit performance sometimes tells only part of the story. It is essential to have actionable business intelligence cross different lines of business and platforms that are capable of dimensional analysis. Only with that can executives have true visibility into their business and make accurate decisions. Information is power; partial information is at best incomplete, and at worst it is misleading.

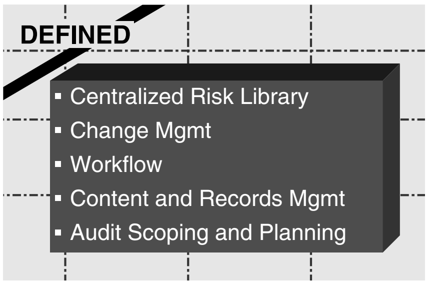
20.5 AUDIT OPERATIONS APPLICATIONS

There are three areas involved in implementing an audit application—namely, the application, content, and implementation. A true end-to-end solution on audit operations should be able to address all three. In other words, the solution should include an application that can be used to address today's pains yet scale to future needs, a set of preseeded content that can be used as a starting point for companies (including a sample risk library and segregation of duties constraints), and a consulting team that can implement the application with optional integration and customization work.

The following section focuses on application requirements for different levels on the maturity curve. Companies should choose an application that can address their pain points today and be scalable to answer tomorrow's needs, especially when the company has a desired higher level in mind.

20.6 STANDARD FUNCTIONALITIES (LEVELS 2 AND 3: DEFINED)

At level 2 (*Defined*), the audit process is defined and documented and all operational processes in the enterprise are standardized. The audit process is repeatable; all processes are documented and can be shared among organizations easily. To achieve this level, the audit operations application should have the following basic standard functionalities:


DEFINED
▪ Centralized Risk Library
▪ Change Mgmt
▪ Workflow
▪ Content and Records Mgmt
▪ Audit Scoping and Planning

- *Centralized risk library.* This is a single repository of processes, risks, controls, audit procedures, and testing steps. Both definitions of and relationships among these objects are stored in the risk library. This way, existing object definitions can be utilized for new mappings. For instance, when a new process is added to the enterprise, existing risks, controls, audit procedures, and testing steps can potentially be reused in mapping to this new process.

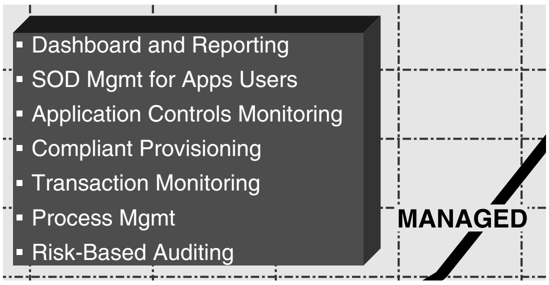
- *Change management.* All objects in the risk library should be under change management. Changes in business are very common. The audit operations application should keep a full audit trail on any changes in the application. The way to ensure that changes are done appropriately is through change management: approval process, versioning, notifications, and change history. This way, changes can be approved, tracked, disseminated, and backtracked.
- *Integration with work flow.* There has to be a work flow or process engine behind the audit operations application. Approval requests, notifications, and alerts can be sent out to appropriate constituents automatically when needed. In addition, a background process definition can mandate the audit process as it is defined in company policy. For example, the company policy could say that whenever there is an audit opinion of "unmitigated" on any risk with high risk exposure (high impact and high likelihood), a finding must be created, assigned, and tracked. The work flow engine can then mandate this policy in the audit operations application by making the auditor fill up a finding template after he/she gives the opinion of "unmitigated" to a risk with high risk exposure.
- *Managing organizations and process structure.* Companies can have very simple or very complex organization hierarchical structures defined in their human resources (HR) systems: lines of business, legal, operational, and so on. There is also the defined master copy of all process hierarchical structures in the risk library. However, when processes are instantiated at different organizations, the structures could have been modified according to local operational needs. All of these predefined structures have to be presented through a simple, easy-to-navigate graphical user interface (GUI). Technologies such as trees can be utilized here. On top of presentations of structures, the audit application should allow end users to create their own organization and process hierarchical structures as part of the personalization feature. Users can then view aggregated data on things like status and progress for their interested areas only. These personalized structures should be created easily with GUIs and drag-and-drop capability and can be shared with other colleagues.
- *Audit projects planning.* Auditing should be done periodically. Sometimes the scope of an audit project is strategic, such as the CFO wants to check control efficiencies in a particular organization because there was a reorganization there last quarter. Other times, the scopes of audit projects are systematic because controls should be tested according to the predefined control testing frequency, controls that are linked to significant accounts should be tested every quarter, or controls that are used to mitigate the risk of company reputation damage should be tested annually. These are all predefined company preferences in testing that mandates scopes of

periodic auditing. The audit operations application should allow scoping, task assignment, and task dependency to be done both manually and automatically through scheduling.

- *Self-assessment support.* Not only auditors test controls, but also business process owners do self-assessments (voluntary control testing) periodically to better understand their processes and improve accordingly. These self-assessments could be done either through surveys and questionnaires or through procedure-based testing like the auditors do. These self-assessment results could help the executives in signing off on their high-level processes and financial statements, along with auditors' testing results. This feature could be seen as a separate application from the audit application because it is utilized by different business users. And companies do keep these activities separated from audit activities. However, the risk library definition could be leveraged here, so that self-assessments that are procedural based could be done without redefining all objects in the risk library.
- *Finding/issue management.* Throughout tests, auditors find trouble areas that should be recorded, assigned, and tracked. Findings and issues are used for this exact purpose. Executives can pay close attention to findings and issues to know what needs to be fixed, who are doing it, and what the progress is in accomplishing it. When findings and issues have due dates, reports like "Past-Due High-Priority Findings" would be good actionable ones for executives.
- *Integration with content management.* All supporting documents of audit operations, such as work papers, process flowchart, and audit opinions evidence, should be stored securely in a content management system. Basic functionalities like version control, security, and check-in/out should be provided to these documents. This integration should be seamless, meaning that shifting between features from audit applications and content management should not be noticeable for users.
- *Data security.* Within an audit operations application, there are many sensitive data. Security is critical in this type of application. Data access management should be done at the most discreet level: role-based security. For example, Peter and Mary can both see the list of control evaluations but, based on their roles in the organization, they will be able to access data differently. If Peter is the owner of the Order to Cash process and Mary is the reviewer on the process, Peter will get to modify data in the audit application, but Mary will only be able to review a view-only version of data in the Order to Cash process.
- *Basic reporting.* Basic online reporting that is downloadable to spreadsheet, PDF, or Word document should be provided for communication purposes.

20.7 ADVANCED FUNCTIONALITIES (LEVEL 4: MANAGED)

At level 4, companies need to have control automation to increase reliability, dashboard, and reporting to measure success and failure. Moving from level 2/3 to level 4 means that companies can realize benefits of cost savings, reliability improvement, and increased visibility by relying more on automated controls, transaction abnormality alerts, and data analysis from different operational areas to resolve problems surfaced in auditing. To achieve this level, the following functionalities are needed in an audit operations application:



- *Audit project management.* More advanced audit project management will improve audit productivity and planning efficiency. Features like milestone tracking, resource management, and Gantt chart presentation should be included here.
- *Automated controls.* This includes three different areas that should be considered, namely segregation of duties (SOD), application controls monitoring, and transaction monitoring.
    - ○ SOD violation means user access to IT systems might have created chances that allow risky events like fraudulent activities to happen. To avoid this, applications should have a set of predefined constraints set up in the system. No new provisioning that violates these constraints can be done without approval. At the same time, existing conflicts in access should be dealt with either by removing certain access or by tracking those users as waived users with documented reasons. Please see the next chapter, “Automation of Segregation of Duties,” for detailed discussion on SOD.
    - ○ There are many embedded controls in business applications’ setup options. For instance, Match Type is a setup value in Account Payables, and it could be a three-way match or two-way match. Depending on company policy on account payables operation, this implementation option should be set accordingly. Application Controls Monitoring allows the IT department to monitor application setup values such as this, and ensure that patch installation and system migration will not deviate application setup values from company policy.

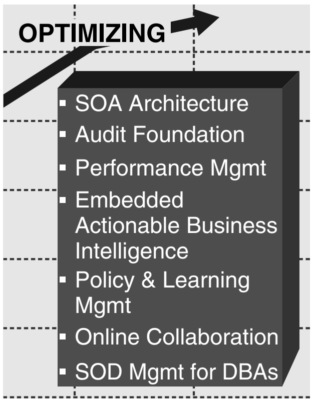
  - Transaction abnormality reporting can catch risks like fraudulent events in advance or shortly after they occur. Apart from abnormality reporting, pattern watching is another way to catch potential problems using the same idea of transaction monitoring. This requires integration with business applications like the ERP system. A rule engine will sit on top of the transaction system for continuous monitoring on all related transactions. If a rule is broken or a threshold is crossed, an alert will be sent to appropriate personnel for further investigation.

- *Dashboard and reporting.* On top of the basic online reporting from the audit applications, more advanced data analysis and aggregation functionalities should be provided for level 4 applications.
  - Aggregated data is needed for senior managers and executives to view progress and status at a higher level. This requires data roll-up on hierarchical structures, such as the organization or process structure. Dashboards are usually the means of delivery. Graphical representation of data is usually preferred for its clearer and easy-to-digest presentation.
  - Detailed reports are then required to provide next-level details. If the executives need to know more on a particular piece of data, they can drill down to the detailed reports for further analysis. At this level of reporting, data should be presented in both graphical and tabular format.
  - Drilling directly into audit applications for actions to be taken is the next level of convenience that the audit operations dashboard can provide. For example, if the number of open findings with high impact on financials in the European Union is unacceptable, and the problem points to a particular finding in France, found by looking at the detail reports, the executives can drill down directly to the audit application to view details on that finding, make comments, and escalate its status if needed. This drill-to-transaction capability is a more advanced feature of dashboards.
  - Another way to help executives to take actions from dashboards is the integration with e-mail systems and online collaborations. Executives need a way to communicate their concerns or have their questions answered quickly. At the dashboard or detailed report level, executives should have the capability to e-mail, call, or chat with someone right there and then. First, the dashboard allows them to know who that someone is, and second, it lets them communicate with that someone right away through whatever means they want. Last but not least, these communications could be tracked through e-mail, online chat text files, or voice files.
  - Auditor-ready reports are the kind of reports that companies can share with external auditors. These are usually reports in PDF format because they are not editable. On top of that format, these reports should also be

easily personalized for column changes, renamed, hide/unhide columns, graph insert, and so on. Companies need to provide whatever data are required by external auditors and should not provide any more or any less. Personalized reports for external auditors enable companies to do exactly that.

20.8 NEXT GENERATION OFFERINGS (LEVEL 5: OPTIMIZING)

At this level, companies need to think about the future quite extensively and they need to change their ways of seeing audit operations applications. Level 5 means that companies are looking for ways to optimize the audit process continuously. Hence, the applications at this level need to be flexible for changes and very adaptive to new business needs. The new way of seeing applications is to have a foundation that carries basic features and can be easily extended to cover advanced requirements by allowing multiple plug-and-play modules. The enabling technology here is a service-oriented architecture where everything is on open standard that allows data extraction and data exchange among all systems through Web services.



- *Audit foundation using service-oriented architecture (SOA).* The basic and advanced requirements for audit applications still stand. The difference is that, at level 5, everything should be on open standard architecture and enable communications with other systems through Web services.
- *Plug-and-play modules.* Because business needs and regulations change over time, customers cannot buy an application today to cover their needs today and for the future. The solution is to have a flexible foundation and allow plug-and-play modules that can address these future needs, whenever they surface, to be easily installed onto and work with the foundation. The following is a list of modules that customers can even consider today:
  - ○ The next generation audit operations applications should be able to import enterprise resource planning (ERP) and/or business intelligence

(BI) sources of quantitative financial data directly and use them as part of materiality analysis on risks and controls, which is part of audit planning.

- Change of regulations should be imported directly from the publishing web sites into the audit operations application for considerations of risks and controls modification and/or change in audit scope.
- Historically, the database administrators (DBAs) or application administrators have had full access to the database, including the application data and the data dictionary, in order to simplify the application implementation and rollout. A very difficult security problem is then to protect application data, sensitive business information, and privacy data related to partners, customers, and employees from DBAs. SOD at database level will restrict the powerful application administrators from accessing other applications and from performing tasks outside their authorized responsibilities. SOD violation detections at DBA level will then become another critical automated control on the audit operations application.
- Provisioning to system access of new users can be done either manually or with an identity management and access management system. A recent popular requirement is to have compliant provisioning. This means that at the provisioning time, a what-if scenario will be created with the new provisioning content, and if the new scenario violates any SOD constraints, the provisioning will be stopped or flagged as an exception. Appropriate personnel will be notified with this new violation. This implies a communication between the audit operations application that stores the SOD rules and the identity management system that does the provisioning.
- Since Sarbanes-Oxley requires a full audit trail on many things, discussions such as those between executives and audit committees certainly should be tracked. Online collaboration systems allow different parties to share documents, comment, request clarification, respond, and reach conclusions at a secured cyberspace. Information and discussion sequence will be kept in the full audit trail. Minutes of these important meetings can be then generated automatically and be attached to the audit application as an evidence of finding disclosure, for instance.
- Policy management systems store policies for the enterprise, and learning management systems disseminate policies to the enterprise and ensure that all employees have looked at them. Any changes to policies will be made in policy management systems and can be made into an online course that all employees should take if the change is significant enough. Once a course is created, all participants' participation status will be tracked. These policy management and learning management

features, by themselves, could be automated controls that are tracked in the audit applications automatically.

Loss events and whistle-blowers are two ways of surfacing problems from within the enterprise by employees. Should anything become suspicious, a case should be created for the legal department to do further investigation. Investigation management systems track cases throughout their life cycles. In audit applications, issues and findings could be turned into cases. The capability of allowing auditors to create a new case and transfer finding or issue details into this new case should be provided through interoperability services between investigation management systems and the audit operations application.

Standard Functionalities

□ Centralized Risk Library
□ Change Management
□ Integration with Work Flow
□ Managing Organizations and Processes Structure
□ Audit Project Planning
□ Self-Assessments
□ Finding/Issue Management
□ Integration with Content Management
□ Data Security
□ Basic Reporting

Advanced Functionalities

□ Audit Project Management
□ Automated Controls: Segregation of Duties (Preventive and Detective)
□ Automated Controls: Application Controls Monitoring
□ Automated Controls: Transaction Monitoring
□ Advanced Dashboard: Dimensional Data Analysis
□ Advanced Dashboard: Drill to Transaction System
□ Advanced Reporting: Auditor-Ready Reports

Next Generation Offerings

□ Service-Oriented Architecture
□ Audit Operations Foundation
□ Plug and Play Modules: Import of Quantitative Financial Data
□ Plug and Play Modules: Direct Import of Regulations Changes
□ Plug and Play Modules: Segregation of Duties at Database Level
□ Plug and Play Modules: Compliance Provisioning
□ Plug and Play Modules: Online Collaboration
□ Plug and Play Modules: Policy Management
□ Plug and Play Modules: Investigation Management

EXHIBIT 20.3 LAUNDRY LIST OF FUNCTIONALITIES

20.9 CONCLUSION

Audit operations have always been a part of daily operations of businesses. U.S. SOX and related regulations simply put this department under the limelight. The question is now how to make auditing more efficient, cost effective, and reliable, yet flexible enough to adapt to a changing regulatory environment. With changes in regulations and business dynamics, audit operations applications should provide basic functionalities with the extensibility and adaptability to become more comprehensive solutions. Companies can use the maturity model to evaluate their current audit process's level of sophistication. Depending on the conclusion of that evaluation, they should pick an application to address their needs of today. However, if they also have a desired level on the maturity model, their current investment should take that into consideration and they should pick an application that can not only solve today's problems, but also be utilized as a comprehensive solution in the long term. Corporations need to think strategically in their application investments today, in order to be able to utilize their existing investment in the future.

For different levels of the maturity model, there are different requirements for audit operations applications. Some applications in the market today package advanced features as part of the basic offerings as well. Exhibit 20.3 is a laundry list of discussed functionalities that should be included in applications at different levels.

Notes

[1] "Study: SOX-Compliant Firms See Drop in Costs in Year 2," by Shamus McGillicuddy, news writer, SearchC10.com, April 21, 2006.