IT AUDIT CHECKLIST SERIES

ComplianceINSIGHT

Risk Management

Practical guidance on how to prepare for successful audits

www.ITCinstitute.com

IT Compliance Institute™

ComplianceINSIGHT

IT AUDIT CHECKLIST SERIES

Risk Management

About the IT Compliance Institute

The IT Compliance Institute (ITCi) strives to be a global authority on the role of technology in business governance and regulatory compliance. Through comprehensive education, research, and analysis related to emerging government statutes and affected business and technology practices, we help organizations overcome the challenges posed by today's regulatory environment and find new ways to turn compliance efforts into capital opportunities.

ITCi's primary goal is to be a useful and trusted resource for IT professionals seeking to help businesses meet privacy, security, financial accountability, and other regulatory requirements. Targeted at CIOs, CTOs, compliance managers, and information technology professionals, ITCi focuses on regional- and vertical-specific information that promotes awareness and propagates best practices within the IT community.

For more information, please visit: www.itcinstitute.com

Comments and suggestions to improve the IT Audit Checklists are always encouraged. Please send your recommendations to editor@itcinsititute.com.

Table of Contents

EXECUTIVE OVERVIEW

What Is the IT Audit Checklist Series?

The ITCI IT Audit Checklists are a series of topical white papers that provide practical guidance for IT, compliance, and business managers on preparing for successful internal audits of various aspects of their operations. In addition to helping managers understand what auditors look for and why, the IT Audit Checklists can also help managers proactively complete self assessments of their operations, thereby identifying opportunities for system and process improvements that can be performed in advance of actual audit.

What Is This Paper About?

This paper, "IT Audit Checklist: Risk Management," supports an internal audit of the organization's risk management program and processes. Providing guidance to improve your risk management program and to assess the robustness of your risk management efforts, the paper is intended to help managers prepare for an audit of risk management, as well as making the audit experience and results as productive as possible.

Paper Contents:

- Organizations are increasingly under pressure to identify all significant business risks they face, and to develop contingency plans and/or manage them to an acceptable level. In addition, with the expanding diversity of risks, a more formalized program of risk management has also become more common-place, generally going under the moniker of an enterprise-wide risk management (ERM) program.
- Everyone in the organization has a role in ensuring a successful ERM program, although management bears the primary responsibility for identifying and managing risk and implementing ERM with a structured, consistent, and coordinated approach. Boards of directors and their non-corporate equivalents have an overarching responsibility for monitoring the risk program efforts and obtaining assurance that the organization's risks are being acceptably managed.
- Internal auditors, in both assurance and consulting roles, contribute to ERM in a variety of ways, such as evaluating the effectiveness of—and recommending improvements to—ERM efforts. Fundamentally, the audit team provides the board and management with an objective and independent assessment of the organization's ERM efforts including what the audit team views as being the key opportunities for improvement.
- The audit's goals, objectives, scope, and purpose will determine the actual audit procedures and questions that are required—modify this "base" IT audit checklist to fit your specific situation. An audit of ERM should determine that the key risks to the organization are being controlled, that the key controls are operating effectively and consistently, and that management and staff have the ability to recognize and respond to new risks as they arise.
- Other resources that complement the paper's thought leadership are provided in the Appendix.

INTRODUCTION TO RISK MANAGMENT

Over the past few years, the importance to corporate governance of effectively managing risk has been widely acknowledged and accepted. Organizations are under ever more pressure to identify their key business risks and to manage those risks at an acceptable level. An expanding universe of business threats, more detailed compliance reporting requirements, and the increasing complexity of business itself all indicate the need for formalized programs of risk management. In many cases, companies are attempting to consolidate all of their risk management efforts into a comprehensive, companywide practice called enterprise risk management (ERM).

Although ERM is integral to compliance with Sarbanes-Oxley (SOX) and Basel II, the regulatory mandate for solid risk management practices goes beyond financial management acts. Growing privacy and security awareness among consumers, companies, media, and elected officials, have prompted the incorporation of risk management best practices into new laws and regulations that define higher operating, security, privacy, and data management standards for organizations. Industry best practices of yesterday are being replaced with legal demands to ensure that organizations' governance, internal controls, network infrastructure, business processes, and operations are safe, sound, and secure. And new laws and regulations dictate (more than ever) how businesses must govern, work, communicate, and securely interact throughout the organization and with external parties such as suppliers, customers, vendors, and strategic partners.

Naturally, as companies dedicate more attention and resources to ERM, the internal audit function follows suit. Internal auditors are increasing the frequency, scope, and "depth" of their assessments of risk management processes and programs.

What Is Enterprise Risk Management ?

According to COSO,[1] Enterprise Risk Management (ERM) is "A process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, manage risk to be within its risk appetite, and to provide reasonable assurance regarding the achievement of entity objectives."

ERM is both an input and output of governance and compliance. As an input, risk management defines tolerances and thresholds that can and should be used to set the scope and focus of compliance functions—both managerial and auditing. As an output, risk management is an auditable and definable set of conditions, procedures, processes, and polices that define a company's ability to recognize and address risk factors.

What Are the Benefits of ERM?

Business is, by nature, fraught with uncertainty. A formal ERM program provides a framework by which a company can more completely understand itself and the environmental factors that act upon its business. The benefits of ERM are thus the business benefits that any company could realize by holistically increasing its self-knowledge and reducing managerial uncertainty.

Many of the most sensational corporate failures in recent years were predicated on risk opacity—the inability of companies to understand the risks that their business practices were incurring and the risk that market and other factors were imposing upon them. In many cases, the problem was not simply that companies did not see risk indicators, but that, even when indicators were apparent, the companies lacked any meaningful way to

[1] The Committee of Sponsoring Organizations of the Treadway Commission (COSO), http://www.coso.org

quantify their potential impact. Moreover, they had no way to reach a corporate consensus on whether specific risks were acceptable or to what degree they should to be mitigated. By contrast, a formal ERM program:

- Promotes a broader understanding of risks across the organization
- Enables board members and other decision makers to recognize risks and formulate appropriate responses
- Tracks what is being done by whom to mitigate observed risks
- Allows decision makers to more quickly recognize and assess emerging risks
- Helps companies to assess and manage risks more quickly than competitors
- Enables companies to evaluate risks in context, realizing when a perceived risk is actually an opportunity

Who Is Responsible for ERM?

The practice of managing risk has traditionally been placed with individual business units or parts of units and, to a lesser extent, distributed across the organization. In contrast, ERM deals with risks and opportunities affecting the creation or preservation of the entire organization's value.

Accordingly, everyone in the organization has a role in ensuring successful ERM, although management bears the primary responsibility for identifying and managing risk and implementing ERM with a structured, consistent, and coordinated approach. Boards of directors and their non-corporate equivalents have an overarching responsibility to monitor ERM program efforts and obtain credible assurance that the organization's risks are being acceptably managed. More organizations are also appointing chief risk officers to give authority and focus to this important long-term effort.

Internal auditors in both assurance and consulting roles contribute to ERM in a variety of ways, such as evaluating the effectiveness of and recommending improvements to ERM processes.[2] Before internal auditors address ERM, however, the entire organization should fully understand management's responsibility for risk management. Auditors' exact roles in relation to ERM depend on the maturity of the organization's efforts. In general, however, auditors:

- Assure management and the board that all that should be done is being done
- Provide guidance on control effectiveness and feedback on managerial decisions and results
- Independently and objectively assess the organization's efforts to protect itself against current and emerging risks

Internal auditors must also take a risk-based approach in planning their audit activities. This approach allows both auditors and the business to focus on efforts and factors that matter most. With limited resources, auditors should focus on the highest-risk project areas and always strive to add value to the organization. Auditors shouldn't make risk-management decisions; their role is to advise and comment on managerial processes and decisions and the organization's efforts.

Organizations that don't have a central ERM program often implement risk management by functional area—or perhaps through several centers of management excellence (for financial risk, commodity risk, market risk, environment health and safety risk, social risk, political risk, supply chain risk, etc.) For such cases, the principles in this paper also apply to those specific departments or risk types.

[2] The IIA International Standards for the Professional Practice of Internal Auditing (Standards) specify that the scope of internal auditing should encompass evaluating risk management and control systems.

THE AUDITOR'S PERSPECTIVE ON RISK MANAGEMENT

Why Audit?

Audits are opportunities for companies to improve, based on auditor analysis and advice. To preserve the integrity and authority of audits, auditors maintain a delicate balance between offering advice and making decisions.

For each company, the parameters of auditor responsibility should be documented in an internal audit charter and approved by the audit committee. According to "The Role of Internal Audit in Enterprise-wide Risk Management," by The Institute of Internal Auditors (IIA), the core internal audit role regarding ERM is, generally, to provide assurance that significant risks are being considered in day-to-day decision making. In providing this assurance, auditors evaluate risk efforts and discuss their findings with management. In addition to evaluating ERM efforts, auditors may also act as champions of ERM by helping managers to identify and evaluate risks, promoting the use of an ERM framework, and advising managers on appropriate tactical and strategic risk management responses.

> An audit litmus test has always been, "Has accountability been established and is it effective and efficient?" Another key audit test is, "Overall, is the program well performing?"

Ultimately, however, business managers, not auditors, must be responsible for risk management. According to the IIA, auditors should not set the company's risk threshold (determine what is and isn't acceptable), dictate risk management processes, implement ERM responses, or make decisions about what responses to make. Each organization has different goals and objectives—and certainly different issues and challenges. There is no one-size-fits-all audit process, nor one audit approach that fits all situations. However, all audit efforts focus on identifying key goals, issues, and challenges, and assessing the organizational efforts to succeed.

At the macro level, audit risk assessments and the development of the audit universe and supporting audit plans should be completed at least annually, and sometimes more frequently. At the micro level, an audit risk assessment of the various entities being audited is completed to support the audit plan (sometimes also referred to as the audit "terms of reference"). Planning for each audit requires thoughtful consideration of the many risks and opportunities facing the organization.

The size and complexity of various organizations' audit efforts are very diverse, due to differences in operating environments, goals, and objectives of each organization. In addition, the scope of audits can also vary from project to project, depending on auditor's focus (e.g., management, technical controls, etc.) This possible diversity of audit focus is another reason management should communicate with auditors early and often for every audit project.

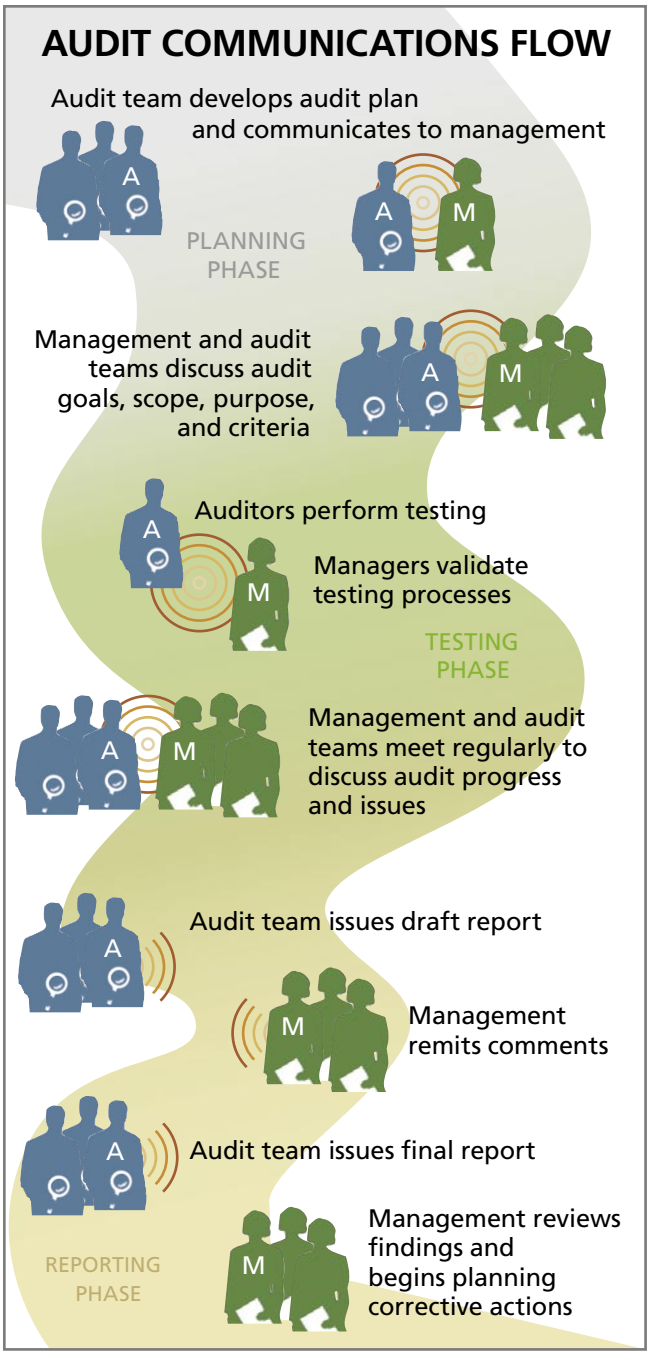
Management's Role in the Audit Process

An internal audit engagement typically has three phases (planning, testing, and reporting) and management has an important role in each phase:

- ☐ **During planning** management should first focus on the audit plan (the auditor's "road map") and come to general agreement with the audit purpose, focus, and approach. An open, positive discussion with the audit team regarding audit goals, objectives, scope, and purpose will help management and the audit team communicate their expectations up front. Such active involvement by management in audit planning is vital to the overall success of an audit. Management should also discuss the evaluation criteria auditors will use in assessing the risk management program. Finally, managers and auditors should broadly discuss planned audit testing, although auditors must have ultimate discretion to select tests they deem appropriate.

- ☐ **During testing** management should confirm audit results (not re-perform the actual tests, but verify processes and data in order to gain confidence in the audit findings). The audit team leader and senior executives (of the business units being audited) should also meet regularly throughout the audit—ideally, weekly and at minimum once a month—to discuss the audit's progress, issues being raised, and potential actions to be taken. An open and transparent dialogue between the senior parties for both management and the audit team does much to avert misunderstandings, or resolve disputed results before audit reporting begins.

- ☐ **During audit reporting** management receives and reviews the findings of auditors, plans and develops corrective actions, and implements change.



Managers and auditors should work together throughout the audit process to ensure that auditors pursue appropriate goals and have proper insight into IT and business processes. Good communication throughout the audit process helps ensure that audit findings are relevant and can be used to benefit the company.

What Auditors Want to See

Audits exist to assess how well a business unit or program meets the performance goals of the organization, as dictated by the CEO, CFO, board, and investors. Accordingly, the managerial goal in auditing is not simply to make auditors happy, but to demonstrate how well operations, controls, and results meet the needs of the business. During audit planning, managers help auditors to design an audit process that truly reflects business strategies and goals. Thus, the managerial response to auditors throughout the audit process—planning, testing, and reporting—is for the benefit of the business, not its auditors.

Auditors exist to provide the board and senior management with an objective, independent assessment of a business unit or program, including what they see as key opportunities for improvement. To prepare their opinions and conclusions, auditors need to review and assess evidence of the risk management program and its performance. Being able to demonstrate performance and show that "accountability" has been established and is working well should make the audit report a positive one (it is that simple).

Accordingly, auditors and managers should work to help each other reach common goals—auditors striving to earnestly, honestly, and completely assess program effectiveness, and management working to help auditors make valid assessments. In that vein, there are some typical program characteristics and managerial processes that auditors do and don't like to see. As in all aspects of audit and risk management programs, auditor likes and dislikes vary by company; however, the following list itemizes typical indicators of good and bad audits.

Auditors Like...

- ☐ Good governance characteristics, such as an ethical culture, atmosphere of open dialog, and absence of fear as a motivator
- ☐ Organized, clear and up-to-date documentation
- ☐ Regular managerial analysis of operating results
- ☐ Management actions based on facts and actual results
- ☐ Documentation of the chain of command and roles and responsibilities, such as up-to-date organization charts and the related job descriptions
- ☐ Timely investigation and clearance of reconciliation items within key accounts
- ☐ Supervisory review of critical performance reports
- ☐ Consistent understanding and use of policy and procedures, from senior management through frontline staff, with no substantial misunderstandings
- ☐ Good management practices—planning, direction, monitoring, reporting, etc.
- ☐ A balance of short- and long-term focus, for both objectives and results
- ☐ Staff development, in terms of knowledge, skills, productivity, and other metrics
- ☐ An engaged workforce and management team

Auditors Don't Like...

- ☐ Interviewing defensive or uninformed managers and executives
- ☐ Wading through piles of disorganized analyses
- ☐ The opposite of the "like" items listed above

How Companies (Inadvertently or Intentionally) Help or Hinder Auditors

Both the audit team and managers should approach every audit process in a positive and open manner. If management and staff are defensive, negative, or even hostile, an audit project can quickly evolve into a no-win, give-no-quarter type of evaluation that ultimately damages every party involved. Even well intentioned management can inadvertently hinder the audit process, however. Management can either help or hinder the audit process by:

- ☐ (Not) having requested documentation available at the prearranged time
- ☐ (Not) meeting deadlines and (not) stonewalling
- ☐ (Not) communicating at an appropriate managerial level
- ☐ (Not) having administrative support where needed
- ☐ (Not) forecasting audit requirements and (not) being overly reactionary to auditor requests
- ☐ (Not) ensuring key staff are available to auditors, especially at critical milestones
- ☐ (Not) informing relevant staff about the audit and its goals, impacting the time and effort auditors must spend to explain the audit to affected personnel

Additionally, executives and senior management can encourage beneficial audit results by ensuring that:

- ☐ The audit team is adequately staffed, according to the needs of the organization
- ☐ An audit charter that defines the mission, scope, authority, accountability, and standards of the internal audit function

Who Should Talk to the Auditors?

An efficient audit process depends on effective communication between auditors, managers, and workers. Management and auditors should strive to balance efficiency (having a minimal number of staff dealing directly with the auditors) with the need for "open access" to management and staff by the audit team (when needed).[3] Obviously, it is impractical and unproductive for both teams to put too many staff in front of auditors. Instead, management should:

- ☐ Provide knowledge of operations through several informed "point" people to interact with auditors. A "short list" of interviewees within the program area being audited can more quickly answer auditor queries and provide better continuity of audit support.
- ☐ Allow ready access to all management and staff, if required by the audit team to gain a clearer picture of overall operations
- ☐ Work with the audit team to draw up a staff interview schedule as part of the planning effort. Update the schedule as necessary during the audit fieldwork phase, if circumstances change.

In many situations, a single point of contact for each audited program will provide the vast majority of documentation to the audit team. The role of that individual—and, indeed, for all auditor contacts—is to ensure that the audit team receives accurate and adequate information for the task. Auditors will still use their professional judgment to determine if and when additional sources of information (other staff interviews) are required. The audit team will also conduct a variety of audit tests, if necessary, to confirm their audit analysis.

[3] The audit team is always expected to ensure all their interactions (with all staff) are professional and result in a minimal disruption.

RISK MANAGEMENT AUDIT CHECKLIST

The audit's goals, objectives, scope, and purpose determine which audit procedures and questions are required. The following checklist describes general audit steps that management might follow in preparation for and during an audit. The list does not attempt to itemize every possible risk management objective, but rather to provide general guidelines about defensible controls and a logical control hierarchy. Modify and augment the checklist below to reflect your own risk environment and situation.

Audit Planning

- ☐ The audit team develops an initial draft of the internal audit plan
- ☐ Managers of the risk management program meet with the audit team
- ☐ Management collects ERM documentation in preparation for the audit team's use
- ☐ Management supports a preliminary survey of the ERM program (by the internal audit team)
- ☐ The audit team finalizes the internal audit plan
- ☐ Management and board members provide feedback on the draft plan

Audit Testing

Processes

Managers support auditors' assessment of the risk management program, as evinced in discussions and documentation.

- ☐ Managers and auditors complete a "kick off" meeting
- ☐ Auditors assess the effect of ERM initiatives on organizational culture
- ☐ Auditors assess the scope and strategy of the ERM program, including how thoroughly it addresses potential risks and compares with evolving industry best practices
- ☐ Auditors examine the structure and resources dedicated to the ERM program, gauging the seriousness of the organization's commitment to effective ERM program management and the program's robustness relative to the potential impact of adverse events
- ☐ Auditors examine management of policies and staff training
- ☐ Auditors survey internal enforcement processes
- ☐ Auditors confirm ongoing efforts of continuous program improvement
- ☐ Managers support a more detailed audit analysis of the risk management program
- ☐ Auditors complete the evaluation of design adequacy
- ☐ Auditors complete the evaluation of operational effectiveness

Steps

The following audit activities may be repeated in each of the aforementioned audit processes.

- ☐ Auditors gain an understanding of the processes and procedures involved with selected activities
- ☐ Managers assist auditors with a walkthrough of selected process
- ☐ Auditors evaluate the quality of risk information generated by the risk management program; the ease, reliability, and timeliness of access to such information by key decision makers; and, finally, the operational consistency with which such information is generated
- ☐ Auditors evaluate performance metrics established for the risk management program: which metrics exist, how they are applied, how often they are monitored, and how deviations are handled
- ☐ Auditors evaluate monitoring metrics for ERM, determine whether they provide useful information relative to the risk objectives
- ☐ Auditors assess whether risk management controls are sufficiently preventive, as well as detective
- ☐ Auditors define tests to confirm the operational effectiveness of risk management activities. Such tests might include interviews with management and staff, documentation reviews, data analysis, assessment of management reporting, and sampling of the results of recent initiatives.
- ☐ Managers provide requested data, documentation, and observations
- ☐ Auditors identify opportunities to improve the effectiveness of risk management activities
- ☐ Managers and auditors complete an exit meeting to discuss all audit findings, auditors' recommendations, and management's response actions

Controls for Risk Management

The controls listed below (and potentially others, depending on the audit's purpose and focus) should be reviewed during the audit planning phase and/or tested. Management should determine the company's actual risk management controls and compare them to the list below. Managers should also periodically assess the effectiveness of key risk management controls and take steps to remediate failing controls.

Management controls to ensure the ERM program is effective and well managed:

- ☐ Risk management program policies and procedures have been established
- ☐ Risk management performance is measured
  - — Performance metrics are established and documented
  - — A monitoring program has been established and is regularly completed by management
  - — Results are evaluated regularly
- ☐ A risk management business plan exists
- ☐ A risk management budget exists
- ☐ A continuous improvement program is in place and operating effectively

Operational controls to ensure that components of the ERM program are operating effectively:

- ☐ Regulatory requirements have been analyzed and operational controls implemented to meet the various requirements, e.g., HIPAA, GLB, etc.
- ☐ Rules and requirements exist and have been documented for specific risk management initiatives and efforts (e.g., treasury financial-risk management controls; IT operational risk management processes and controls, and so forth)
- ☐ Staff adherence to risk management policies and procedures are regularly and formally evaluated
- ☐ A supervisory review of key management reports and operating results occurs regularly

Technical level controls to ensure that ERM systems are effective and efficient:

- ☐ Privacy- and security-related controls have been defined and are operational
  - ___ User access controls exist for critical computer applications
  - ___ User access controls exist for databases and other repositories of sensitive data
- ☐ The effectiveness of privacy and security controls is regularly tested

Audit Reporting

During the reporting phase, management and the board of directors receive formal feedback from the audit team. This knowledge transfer should be an open and transparent process. Almost every audit identifies opportunities for improvement. The key goal of management and auditors should be to first address critical issues, followed by important issues. Both management and auditors should work to ensure that, whatever action plans they agree to, the goals are achievable and beneficial to the organization.

The following are typical steps an audit team takes to confirm and release the audit results.[5]

- ☐ Auditors debrief management, formally discussing significant audit findings and conclusions before they issue the final audit report
- ☐ Managers receive a written draft report from auditors
  - ___ The report communicates audit results clearly and precisely
  - ___ Results are presented in an unbiased tone, noting where management has taken actions to correct deficiencies and acknowledging good performance
- ☐ Management and auditors discuss the draft report
- ☐ Management provides feedback on the draft report
- ☐ Auditors review managerial comments and action plan(s)
- ☐ Auditors finalize and distribute the final audit report
- ☐ Auditors close out the internal audit project and plan any necessary follow-up efforts regarding management's action plans

Auditors might also choose to communicate some audit findings that might be useful for risk management efficiency and effectiveness, but do not warrant including in the formal report. This type of communication should be documented, if simply as a note in audit findings that a topic was verbally discussed with management.

[5] In organizations with established internal audit functions, there may be standard operating procedures (SOP) for audit reporting (and other audit activities). If so, these audit SOPs should be reviewed and understood by management.

PREPARING FOR AN INTERNAL AUDIT

A well managed business unit or risk management program includes robust plans, procedures, goals, objectives, trained staff, performance reporting, and ongoing improvement efforts. The internal audit team looks for evidence that the business unit and risk management program is well organized and well managed.

While the audit is in the planning phase, management must be very proactive when working with the audit team and must "educate" the auditors. Expectations are a two-way street, and management needs to work with the auditors to ensure that both sides are working together and understand each other. Business managers should be prepared to provide auditors with a well-documented description of the business unit/program including its key policies, procedures, and ongoing efforts (key initiatives, for example) to succeed. This entails, ideally, providing the auditors with robust business plans, with supporting budgets, the policy and procedures manual(s), the assignment of responsibilities (such as up-to-date job descriptions), results reporting and other trending information, and finally, any other relevant guidance (to management and staff) that demonstrate a "well-run" and performing business unit and program.

The goal of providing this documentation is not to overload the audit team with information, but rather to provide insight into how the business and risk management program is run and how well they are doing. The business unit and program's periodic risk assessment is another key management document to be shared with the auditors. While an audit is still in its planning phase, managers should make an active effort to:

- ☐ Learn early and contribute often to the internal audit goals, objectives, purpose, approach, and procedures (audit tests). In particular, setting an appropriate purpose and the audit approach are the two most important elements of every successful audit.
- ☐ Discuss with audit management the evaluation criteria and standards and how the audit will actually be conducted, in order to ensure that you'll receive a quality audit. Ask whether they audit in accordance with international standards for the professional practice of internal auditing.
- ☐ Learn who is on the audit team and their qualifications, talents, and motivations. The audit team exists to help make your operations more efficient and effective, but they are also individuals with strengths and weaknesses common to many employees. It pays to know the experience of your auditors, whether they're rookies or veterans (and perhaps to push for the latter). Showing an interest in their work can also influence and increase the benefits from the audit—within reason. At the end of the day, auditors still need to be independent and objective.

During all of its discussion with the audit team prior to the audit, management should try to strike a balance between influence and deference. Managers should neither entirely yield to the audit team nor micromanage their efforts. A good interaction policy is to provide constructive input on the evaluation methodology before audit management approves it.

EFFECTIVELY COMMUNICATING WITH AUDITORS

Like any interaction between people, but particularly in the work environment, a professional and trusting relationship is a strong precursor to successful collaboration. When management interacts with the auditors in a professional manner, it tells the audit team that its function is respected and supported. Likewise, lackadaisical efforts by management and staff reflect poorly on the business unit or process, its capabilities, and its performance. Management should also expect professional interaction from the audit team and push back whenever they see an exception to this practice.

- ☐ Understanding that the nature of the judge/judgee relationship can often become emotionally charged, each participant should make a conscious effort to demonstrate objectivity, responsiveness, and listening skills. An upfront investment by management and the audit team to fully understand each other's needs and expectations will pay off with clear expectations contributing to good results.

- ☐ In particular, management should be open and receptive when discussing audit observations and recommendations. As the testing phase concludes, the audit team prepares summaries of its key findings. The business unit management should be prepared to provide feedback and comments on these summaries prior to the final, formal audit report. The audit report often forms the basis of future IT and business initiatives. With time and development resources on the line, management should ensure that every audit point raised (and its related recommendation) is worthy of mention and that every action plan proposed by management or audit is achievable, appropriate, cost effective, and capable of effecting lasting impact.

- ☐ In particular, if managers feel the draft report is incorrect, they must speak up, and auditors should be receptive and responsive to this managerial feedback. Ultimately, managers—not auditors—are responsible for implementing responses to the issues raised in the audit. Leaving misunderstandings and unresolved issues on the table to be codified into the final audit report is tantamount to failing the goals of the audit itself. Finally, for the good of the total business, executives should encourage a "partner" relationship between audit and managerial teams.

APPENDIX—OTHER RESOURCES

1. **The Committee of Sponsoring Organizations of the Treadway Commission** (COSO); http://www.coso.org
2. **Unified Compliance Project: Audit and Risk Management**; IT Compliance Institute (ITCi); http://www.itcinstitute.com/ucp/arm
3. **The Role of Internal Auditing in Enterprise-wide Risk Management**; the Institute of Internal Auditors (IIA): http://www.theiia.org/iia/download.cfm?file=283 (PDF)
4. **Control Objectives for Information and Related Technology** (COBIT); ISACA: http://www.isaca.org/cobit
5. **"Auditing System Conversions"**; the IIA: http://www.theiia.org/ITAudit/index.cfm?act=itaudit.archive&fid=5495
6. **NIST 800-30: Risk Management Guide for Information Technology Systems**; National Institute of Standards and Technology (NIST): http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (PDF)
7. **Internal Audit Guide (IAG): Evaluating and Compliance and Ethics Program**; Open Compliance and Ethics Group (OCEG): http://www.oceg.org/landing/IAG.aspx
8. **"The Easiest and Best Matrices for Documenting Internal Controls"**; Matthew Leitch: http://www.managedluck.co.uk/matrices

ABOUT THE AUTHOR

Dan Swanson, CMA, CIA, CISA, CISSP, CAP

Dan Swanson is a 24-year internal audit veteran, who most recently was director of professional practices at the Institute of Internal Auditors. Prior to the IIA, Swanson was an independent management consultant for over 10 years. Swanson has completed internal audit projects for more than 30 different organizations, spending almost 10 years in government auditing, at the federal, provincial, and municipal levels, and the rest in the private sector, mainly in the financial services, transportation, and health sectors. The author of more than 75 articles on internal auditing and other management topics, Swanson is currently a freelance writer and independent management consultant. Swanson recently led the writing of the OCEG internal audit guide for use in audits of compliance and ethics programs (www.oceg.org) and participated in the COSO small business task force efforts to provide guidance for smaller public companies regarding internal control over financial reporting (www.coso.org). Swanson is a regular columnist for *ComplianceWeek* and also writes the ITCI "Auditor Answers" column.

Comments and suggestions to improve the IT Audit Checklists are always encouraged. Please send your recommendations to editor@itcinsititute.com.