HABITS OF A HIGHLY EFFECTIVE AUDIT FUNCTION

Keith Bujalski

FIRMA National Risk Management Training Conference

April 23, 2018

Internal Audit Charter

Authority

- The Internal Audit function should have full, free, and unrestricted access to any and all of the organization's records, physical properties, and personnel pertinent to carrying out any engagement. The Internal Audit function should also have free and unrestricted access to the Audit Committee of the Board of Directors.

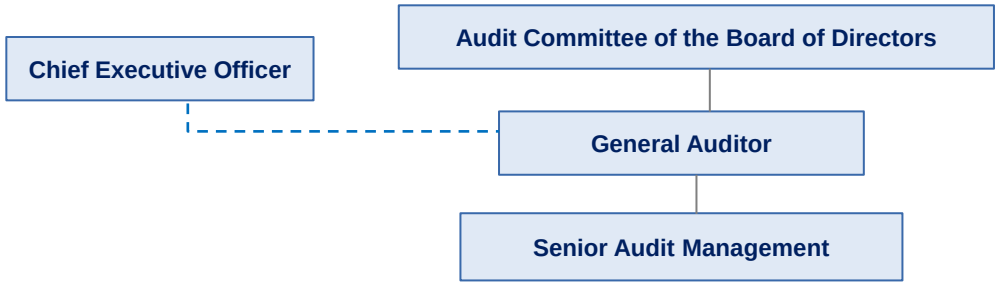
Professionalism and Independence

- The Internal Audit function should govern itself by adherence to The Institute of Internal Auditors' Mandatory Guidance, which includes the Core Principles for the Professional Practice of Internal Auditing, the Code of Ethics, and the International Standards for the Professional Practice of Internal Auditing, and the Definition of Internal Auditing. This constitutes principles of the fundamental requirements for the professional practice of Internal Auditing and for evaluating the effectiveness of Internal Audit's performance.

- Internal Audit resources should adhere to the firm's Code of Conduct and other relevant employee related policies and procedures, and Internal Audit's standard operating policies and procedures.
- To provide for the independence. the Internal Audit function should:
  - Report functionally to the Board and administratively to a senior executive of the organization i.e., the Chief Executive Officer.
  - Communicate and interact freely and directly with the Board, including in private sessions and between Board meetings, as appropriate.
  - Confirm to the Board, at least annually, the organizational independence of the Internal Audit function.
  - Update and review the Internal Audit Charter with the Board, at least annually, for their approval.
  - Submit to the Board, at least annually, an Internal Audit plan, financial budget and resources, and overall audit methodology for review and approval.
- The Internal Audit function should remain free from interference with respect to matters of audit selection, scope, procedures, frequency, timing, and report content to permit maintenance of a necessary independent and objective approach.
- Internal Auditors should not perform any operational duties for the organization or its affiliates or direct the activities of any employee not employed by the audit department.
- Internal Auditors should exhibit the highest level of professional objectivity in gathering, evaluating, and communicating information about the activity or process being examined.
- Internal auditors should make a balanced assessment of all the relevant circumstances and not be unduly influenced by their own interests or by others in forming judgments.

Internal Audit Charter (continued)

Organization Reporting Lines



Responsibility

- The scope of Internal Auditing should encompass, but may not be limited to, the examination and evaluation of the adequacy and effectiveness of the design of the organization's governance, risk management, and internal control processes as well as the quality of performance in carrying out assigned responsibilities to achieve the organization's stated goals and objectives. This should include:
  - Evaluate the controls established to ensure compliance with new and existing policies, procedures, laws, and regulations which could have a significant impact on the organization.
  - Develop an annual audit plan using an audit methodology which considers and assesses each auditable component of the company.
  - Report periodically on Internal Audit's purpose, authority, responsibility, and performance relative to its plan, including the status of results of the Internal Audit program, significant control issues identified, emerging themes, and the overall adequacy of the control environment.
  - Report significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by the Board.
  - Evaluate specific operations, as appropriate, including assisting in special investigations regarding errors, irregularities, internal controls, improper employee conduct or fraud at the request of the Board or management.
  - Maintain professional audit resources with sufficient knowledge, skills and experience to perform their responsibilities.
  - Identify situations where external assistance is required to augment existing Internal Audit skills and/or resources, under the supervision and review of Internal Audit staff. In the event outsourcing may be required, the General Auditor should approve the arrangement and obtain approval from the Board for any Internal Audit engagements above a reasonably pre-defined expense threshold.
  - Demonstrate high integrity when dealing with regulators, and remediating any issues relevant to Internal Audit raised by these parties in a constructive, open fashion.
  - Communicate and coordinating with external auditors, as appropriate.

Independence of Audit Staff

Staff Independence

- While the reporting line of the Internal Audit function should provides the framework within which the audit process can be carried out with independence, the actual attainment of independence is contingent on the objectivity of each member of Internal Audit.
- In order for internal audit activity to be independent, internal auditors must be objective in performing their work.
- If independence or objectivity is impaired in fact or appearance, the details of the impairment must be disclosed to appropriate parties.
- It should be the responsibility of the internal auditor to have an impartial, unbiased attitude and avoid any conflict of interest.
- A policy should exist whereby all employees and contractors are required to annually affirm their compliance with independence requirements, as well as make any necessary disclosures to identify the relationships, activities, or circumstances (real or perceived) which could contribute to a conflict of interest.

Skills Assessment of Audit Staff

Skills Assessment Process

- A Skills Assessment should be conducted annually to evaluate whether Audit resources have the experience, knowledge and skills commensurate with their roles and responsibilities.
- The information collected in the Skills Assessment will allow the senior audit management and the General Auditor to identify skills needs and associated gaps that could potentially be resolved through training, targeted hiring, realignment, or resource sharing across the Internal Audit department.
- The Skills Assessment should include questions that assess overall knowledge and skills (e.g., professional experience, core audit competencies, professional skills).
- It may also incorporate additional questions for assessing specialized product knowledge and skills (e.g. Anti-Money Laundering, Fiduciary, etc.), as needed.
- Subject matter experts should be involved in drafting the questions and determining the populations for any separate, specialized questionnaires.
- An executive summary and the results of the Skills Assessment should be presented to senior audit management, including the General Auditor, and the Audit Committee annually.

Annual Planning and Risk Assessment

Audit Universe

Overview

- The audit hierarchy should be aligned to the organizational management, finance, and control self assessment hierarchies of the organization.
- A comprehensive audit universe should be the foundation for development of the annual plan. Internal Audit should follow a process to understand the firm's business and risks to define and maintain the audit universe.

Auditable Entities (AE)

- The audit universe represents the aggregation of all auditable components across the organization. An Auditable Entity is typically defined as the lowest level entity for which Internal Audit would reasonably perform a risk assessment on a standalone basis and highest level at which an audit would realistically be performed.
- Typically, an Auditable Entity can be defined as:
  - Key business and/or technology processes
  - Functional or operational units
  - Key products or services

Risk Assessment

Overview

- Internal Audit should perform independent risk assessments annually for all Auditable Entities within each business activity and corporate function. Risk should be measured relative to the firm using consistent assessment criteria. Inherent risks should be evaluated based on pre-established risk categories. The determined inherent risk can be reduced by control effectiveness ratings to derive an overall risk rating.

Audit Cycle Coverage Framework

- Auditable Entity risk ratings should drive a frequency requirement relative to the risk rating assigned. For example, the risk rating categories and associated audit frequency can be as followed with the higher risks to the firm being audited more frequently:

AE Risk Rating	Frequency
High Risk	Annual
Moderately High Risk	2 years
Medium Risk	3 years
Low Risk	4 years

Annual Planning and Risk Assessment (continued)

Risk Assessment Categories

- The following are examples of risk categories to consider when determining inherent risk of an Auditable Entity:
  - Credit
  - Fiduciary
  - Finance
  - Fraud
  - Market
  - Model
  - Operational
  - Regulatory/Legal/Compliance
  - People
  - Strategic
  - Technology

Annual Audit Plan

- The annual plan should also consider the following:
  - Performing a broad organizational analysis to identify areas that require coverage regardless of the results of the risk assessment (e.g., most significant risks, thematic control issues, strategic priorities, certain locations, etc.)
  - Identifying regulatory required audit coverage and change activities to be performed
- A projected forecast should be performed over the longest cycle for coverage of the audit universe based on the results of the risk assessments. Each Auditable Entity should be subject to audit coverage of key risks within the relevant risk-based frequency requirement.
- The annual audit plan should be approved by senior audit management, including the General Auditor. The final annual audit plan should be submitted to the Audit Committee of the Board of Directors for approval annually.

Audit Execution and Reporting

Overview

- Audit engagement activities are typically split into Planning, Fieldwork, and Reporting cycles as described below:

Planning	Fieldwork	Reporting
▪ Identify key risks and controls applicable to the Auditable Entity under review through process walkthroughs ▪ Determine and agree audit scope	▪ Perform testing to evaluate the design and effectiveness of controls that are in place to mitigate the applicable risks relevant to the scope of the audit ▪ Identify any related issues	▪ Determine severity of all identified issues and obtain action plans ▪ Determine audit report rating

Audit Activity Types

Type of Activity		Definition
AE Coverage	Audit	■ Examination of significant business and operational key risks and the controls established to mitigate those risks, including compliance with laws, regulations and established policies and procedures ■ Includes horizontal audits conducted on one topic, process or function across multiple businesses and/or corporate functions
	Targeted Control Review	■ Focused on a select group of key risks and controls to allow Internal Audit to quickly assess and communicate whether key controls are operating effectively or require remediation ■ Generally completed within a short period of time i.e. 30 days or less
	Post-Acquisition Review	■ Performed upon the purchase of an entire company, a portfolio from another business, the in-sourcing of a business process from another company, or participation in a joint venture to assess the control environment of the acquired company/process in relation to the acquiring organization's standards ■ Follow-up reviews should be performed on initial post-acquisition reviews, generally within six months of report issuance
Change Activity		■ Encompasses any event with significant impact on the control environment, including new products/ businesses, new/significantly revised regulations, new accounting pronouncements, large-scale remediation programs, system development/implementation, business migrations/consolidations, business divestitures and branch/office closures ■ May include participation in key governance forums, evaluation of the overall governance structure, review of critical project documentation, review of business requirements and participation in readiness reviews
Investigation / Post Mortem		■ Investigations are conducted following control breakdowns related to internal/external frauds or instances of employee misconduct. Internal Audit engagement is generally in partnership with the firm's corporate security department and/or Legal. ■ Post-mortems are event-driven activities conducted on business processes, generally after significant control breakdowns, to determine root cause and lessons learned. Post-mortems should be conducted at the direction and discretion of the General Auditor.

Audit Execution and Reporting (continued)

Audit Execution Governance

Tollgates

- Internal Audit tollgate meetings should be held during each of the phases (planning, fieldwork and reporting of an audit to ensure audit activities are appropriately planned and scoped, work progresses as planned, and results are appropriately framed, documented and communicated at the conclusion of the project.
  - Planning Tollgate - The planning tollgate meeting should be held prior to the issuance of the Announcement Memo and the beginning of fieldwork. Its purpose is to ensure the project is properly staffed and focused on the highest risks, audit staff has a detailed understanding of the area/process, and testing/coverage strategies are appropriate. Additionally, a communication plan, for both the audit team and the stakeholder, should be developed during the tollgate meeting.
  - Fieldwork Tollgate - The fieldwork tollgate meeting should held when a significant portion of the audit fieldwork is complete. The objective of the meeting is to determine if the audit is progressing as intended and to make adjustments to strategy, scope and staffing as required. Also at this meeting, potential issues, issue severity ratings, supporting evidence, root cause, control condition, culture and conduct, and impacted region should be discussed to ensure they are appropriately dispositioned and communicated.
  - Reporting Tollgate - The reporting tollgate may be held late in fieldwork or after the conclusion of fieldwork, but prior to final report issuance. The objectives of the meeting are to determine if issues are dimensioned appropriately and management of the business being audited is engaged and providing action plans for the reportable issues, and to review the draft Internal Audit report and determine the audit rating.

Workpaper Supervision

- The auditor in charge of an engagement should be responsible for monitoring and managing the progress of the audit. They should also be responsible for conducting the initial review of all workpapers. A final quality check of all workpapers to verify proper completion and review in accordance with industry standards should also be performed.
- The auditor in charge should be responsible for providing oversight for the proper completion of audit documentation and required to specifically review key documents within the workpapers. In addition, any worked performed by the auditor in charge should be independently reviewed by another manager who has sufficient knowledge of the area under review.
- All workpapers are to be reviewed and approved by at least one person other than the preparer. All workpaper reviews should be completed prior to the issuance of the final report.

Audit Execution and Reporting (continued)

Reporting - Issue Dimensioning

- Internal Audit issues should be dimensioned based on severity i.e. *High, Medium, or Low* considering the following.

HIGH SEVERITY	***MEDIUM SEVERITY***	***LOW SEVERITY***
An issue that poses significant risk to the business or function and requires immediate remedial attention by management. This issue has either resulted in, or could result in any of the following impacts: • Significant financial loss • Significant regulatory issues • Significant violation of firm policies or values • Material impact on our ability to provide services to our clients/customers or employees • Disputes, litigation, or offenses resulting in substantial damages, costs, or fines • Derogatory press coverage or significant reputational harm • Damage to brand that could result in significant loss of customers or market share	An issue that represents weaknesses in the control environment for the line of business or function and requires timely attention by management for corrective action. This issue has either resulted in, or could result in any of the following impacts: • Errors or incidents • Some financial or reputational harm • Regulatory scrutiny	An issue that poses negligible financial, legal, regulatory, or reputation impact.
Issue severity ratings should be based on the impact of the control deficiency and the likelihood of occurrence. Likelihood can reflects past and future occurrences.		

- **Likelihood** of occurrence includes a percentage for probability and time horizon and should based on the following:
  - Control design (i.e., is this considered a systemic issue or an isolated exception?)
  - Control condition (i.e., missing control, control design weakness, or ineffective control execution)
- **Impact** of the issues can be quantitative, qualitative, or both:
  - Quantitative financial measurement for impact include specific dollar targets attributed to profit, loss, revenue, or expenses
  - Qualitative factors client/legal, regulatory, reputational, and policies and procedures
- Severity rating should be based on the residual risk and the impact that the control break will have on the control environment
- Manually intensive processes can be more susceptible to errors and/or fraud and may negatively impact the control environment
- Issue dimensioning should apply to Internal Audit, business, regulator, and external audit identified issues within the scope of the audit

Audit Execution and Reporting (continued)

Reporting - Ratings

- The audit rating should reflect the design, effectiveness, and sustainability of the controls within the scope of an audit, not the line of business or firm as a whole. Audit ratings should reflect the view of the control environment at the time of the audit. Control deficiencies corrected prior to report release should be considered issues for the purpose of the audit rating.
- Significant repeat issues should be considered for potential rating downgrade.
- The primary root cause and control condition should be reported for all identified key issues.
- Audit observations related to the effectiveness of Management's self assessment process, including commentary on the governance, inherent risk (composition and rating), control effectiveness (composition, substantiation and design, and ratings) and residual risk for the self assessment in scope, should be considered for inclusion in each audit report where applicable.
- Audit ratings should reflect three core elements: design, effectiveness and sustainability of the control environment, isue management and risk mitigation; and risk management:
- A typical three tier rating scale can resemble the following:

SATISFACTORY	***FAIR or NEEDS IMPROVEMENT***	***UNSATISFACTORY***
Internal control processes and systems are effective and operating as designed. The number and/or nature of issues relative to the size and scope of the audit were isolated to moderate areas of weakness in the controls. Risk management processes are effective.	Most internal control processes and systems are designed and/or operating effectively. Some areas need management attention. The number and/or nature of issues relative to the size and scope of the audit indicate certain control weaknesses could result in increased exposure. Risk management processes may need to be enhanced.	Internal control processes and systems are not designed or operating effectively and require immediate management attention. The number and/or nature of issues represent a pervasive or significant breakdown of key controls resulting in unacceptable levels of risk. Risk management processes are not effective.
Controls included in the scope of an audit and any related issues, regardless of how identified, should be considered in determining the overall audit rating.		

Other Audit Activities

Issue Closure Validation

- Audit should perform validation on internal audit and regulator identified issues within a reasonable periodic of time i.e. 60 days of issue closure
- Sufficient testing should be performed to ensure appropriate remediation of issues has occurred.
- Timeliness of audit validation work should be tracked and reported to senior audit management.
- For any issue found to be less than fully remediated, formal reporting should be provided to business management who own the issue. The reporting should describe the unresolved, or new, issue(s) and related action plans, and addressed to the senior business manager accountable for resolving the issue, similar to the protocol used for the audit reporting process.

Continuous Monitoring

- Continuous monitoring should be a component of audit coverage and the ongoing evaluation the organization's business activity and risk profile.
- It is should be designed to trigger the need for future audit plan and risk assessment adjustments to address the changing risk profile of the firm, impact scope on future audits, or highlight an audit identified issue.
- Continuous Monitoring activities may include:
  - Analysis, trending and investigation of key business MIS and supporting activity
  - Participation in oversight committees (e.g., control forums, business control or risk committee meetings)
  - Meeting with senior management of the business and other corporate or control function
  - Assessment and monitoring of key business risks and performance indicators, such as key financial data; review and analysis of system capacity, resiliency, system outages, etc.; review and analysis of business scorecards highlighting changes or unusual trends; and review and analysis of business changes, including new business activities, management/organizational changes, and regulatory changes, etc.
- Key components of the Continuous Monitoring framework should be the strategy, execution and summary of results.
  - Strategy documents describe the approach and should be revisited when significant changes occur to the business or risk model.
  - Event documents should be created when Audit become aware of events (e.g., material errors/issues; significant business initiatives and organizational changes; significant system/ infrastructure changes; significant changes to key metrics; significant regulatory developments; delayed action plans; cross business and emerging risks related topics) requiring further follow-up
  - Events should be tracked to resolution and what (if any) Audit action the event resulted in.

Management and Audit Committee Reporting

Management Reporting

Firmwide Reporting

- Summaries of audit activities should be communicated monthly to senior business management, risk and control forums, and the Audit Committee. Audit activities reported should include the following:
  - Unfavorable Rated Audits
  - Audit Report Rating Distribution
  - Audit Issues (new, resolved, aged, and repeat issues)
  - Audit Issues Outstanding and Audit Issue Validation Trends
  - Regulatory Issues Outstanding and Issue Validation Trends
  - High Severity Issues
- Results should be provided for each line of business and corporate function.

Audit Committee Reporting

- The Audit Committee should be regularly apprised of the annual audit plan, including significant interim changes and performance relative to plan as well as audit results, outstanding issues, issue validation trends, issue themes, summary of key audits, other key department activities and resources.
- On an annual basis, Audit should present their overall plan of audit coverage for the year. This includes the following information:
  - Planned coverage for each line of business and corporate function
  - Current year financial plan and prior year results
  - Resource requirements
- Performance relative to the annual plan, as well as significant changes to the plan. should also be communicated to the Audit Committee periodically.

Internal Audit Quality Assurance Program

Quality Assurance (QA) and Improvement Program

- Internal Audit should maintain a quality assurance and improvement program that covers all material aspects of the Internal Audit function. The program should also assess the efficiency and effectiveness of the Internal Audit function and identify opportunities for improvement.
- The General Auditor should communicate to the Board on Internal Audit's quality assurance and improvement program at least annually, including results of ongoing internal assessments and external assessments (which may be required at least every five years) and the qualifications and independence of the assessment team, including potential conflict of interest.
- The QA program should be an end-to-end approach encompassing all activities of an audit function, including:
  - Audits
  - Audit and Regulatory Issue Closure Validations
  - Continuous Monitoring
  - Change Activities
  - Risk Assessments
- Objectives of the QA program should be to:
  - Evaluate the adequacy, effectiveness, and efficiency of the audit process, specifically including assessing adherence to Internal Audit policies and the Institute of Internal Auditors standards
  - Assess the adequacy of audit coverage across the audit universe.
  - Substantiate the appropriateness of risk identification and scoping decisions
  - Validate conclusions (includes individual test conclusions, as well as overall audit ratings)
  - Assess the quality of documentation across all audit activities; determine that work is defensible
  - Confirm appropriate supervisory involvement and review
  - Provide an independent opinion on the adequacy of audit activities
  - Identify best practices and opportunities for improvement
- Framework
  - QA reviews should be completed by an independent centralized QA team
  - All Internal Audit teams should be subject to a QA review on a minimum cycle basis
  - Provide formal QA reporting of any nonconformance with Internal Audit policies and/or IIA standards
  - Provide summary reporting to senior Audit management, including the General Auditor, and the Audit Committee periodically