Larry's Cheat Sheet – Doing QAR's

Best Practices in Doing QAR's

- Use a Maturity Model to rate status of IAD's maturity WRT the Standards, and their compliance with Standard 1300.
- Use electronic questionnaires for management and staff surveys – Survey Monkey is good.
- Do workpaper reviews remotely, before going on-site.
- Rate IAD vs. The Standards, not vs. what you do. Keep asking, "What do the Standards say?"
- Go to lunch with auditors every day.
- Self-Assessment with Independent Validation (SAIV) is best way to do satisfy Standard 1312.
- Have all external reviewers working in same room during the review.
- Use The IIA Quality Assurance Manual Tools, but only with care.

Best Practices for IAD's

- Have corporate policy regarding responsibilities for fraud
- Have corporate policy regarding internal control
- Track ex-IAD members, so they feel alliance with IAD
- Provide training in internal controls and risks on every audit
- Analyze actual audits done in a year vs. the planned audits at start of year
- Use full Balanced Scorecard for metrics: Clients, Process, People, and Internal Control Status.
- Reimburse for CIA Exam and any other review courses (CFE, CISA, CCSA), once Exams are passed.
- Use a Residual Risk format of Risk/Control Matrix
- In Audit Reports:
  - Have final draft of audit report available at end of fieldwork.
  - Link findings to COSO components that failed.
  - Use "Action Plan" narrative instead of separate "Recommendations" and "Management Comments."
  - Use a Maturity Model to rate status of internal controls in audited areas.
  - "Risk rating" of audit issues is very subjective.

Internal QAR's

Both ongoing and periodic should be in place:

- Ongoing - Engagement supervision, checklists, feedback from audit customers, budgets/timekeeping, metrics
- Periodic – Self-assessment of compliance with Standards, reviews of effectiveness and efficiency of the IA activity

Possible Outcomes, as Used By IIA

GC — "Generally Conforms" - the relevant structures, policies, and procedures of the IA activity, as well as the processes by which they are applied, comply with the requirements of the individual Standard or element of the Code of Ethics in all material respects.
PC — "Partially Conforms" – the IA activity is making good-faith efforts to comply with the requirements of the individual Standard or element of the Code of Ethics, section, or major category, but has fallen short of achieving some of their major objectives.
DNC — "Does Not Conform" – the IA activity is not aware of, is not making good-faith efforts to comply with, or is failing to achieve many/all of the objectives of the individual Standard or element of the Code of Ethics, section, or major category. These deficiencies will usually have a significant negative impact on the activity's effectiveness and its potential to add value to the organization.

Tips for External Validators or QAR Teams

- Don't confuse independent with objective, or conformance with compliance.
- In SAIV, be sure following are ready and available BEFORE going on-site: self-assessment report, evaluation of compliance by Standard, workpaper reviews, issues sheets, interviews scheduled.
- Need access to electronic workpapers, audit manual, etc.
- If client and management feedback is already being received, use that instead of separate QAR surveys.
- SAIV validator assesses the "process" IA used in self-assessment. IA does the full evaluation, report and assessment and validator adds their concurrence.
- Keep the Three Lines of Defense Model in mind. (2013 Position Paper)

Management and Board Interview Points

- Purpose of QAR
- Attitude and policies toward risks and controls
- Objectivity, credibility, effectiveness of IA activity
- Other comments about IA, controls, risks or governance.

Audit Customer Surveys

- Relationship with management
- Scope of audit work
- Management of audit activity
- Audit staff professionalism
- Audit process
- Value added

QAIP Maturity Model From IIA

- **LEVEL 1: Introductory:** The internal audit activity does not have a Quality Assurance and Improvement Program in place. Typically, a level-1 internal audit shop would be fairly new or one that has not yet conformed to the new requirements. In some cases the CAE and audit committee might not have a clear understanding of the importance of such a program and the value it can bring to an organization.
- **LEVEL 2: Emerging:** The internal audit activity conducts periodic and ongoing self-assessments, or internal quality assessments (QA's), monitoring compliance with the Standards.
- **LEVEL 3: Established:** The internal audit activity obtains an independent validation of its self-assessment and will do so every five years.
- **LEVEL 4: Progressive:** A Quality Assurance and Improvement Program is well defined within the ongoing operations of the internal audit activity. The activity generally complies with the Standards and Code of Ethics, and obtains an external QA every five years.
- **LEVEL 5: Advanced:** An active and fully integrated Quality Assurance and Improvement Program exists within the daily operations of the internal audit activity. The activity obtains an external QA every three years. All staff members follow a rigorous continuing education program.

Larry@LHubbard.com

Larry's Cheat Sheet – Doing QAR's

Code of Ethics – Principles and Rules of Conduct related to Integrity, Objectivity, Confidentiality, and Competency for individuals and entities that provide internal auditing services.

Definition - Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

Common Problems in QAR's

- More than 95% of all QAR's are rated GC overall – nobody fails a QAR.
- Rate vs. the Standards, not vs. what the QAR Team has seen.
- In RFP, to evaluate flexibility of QAR Team, ask:
  - If audit department and Team disagree whether or not something is in accordance with the Standards, how will the issue be decided and reported?
  - If something is in accordance with the Standards, but Team thinks it could be done better another way, how will it be decided and reported?
  - If audit department already gets client feedback after audits, will Team still need to do surveys?

- 1000 – Purpose, Authority, and Responsibility – Charter not being up-to-date.
- 1010 - The mandatory nature of the Definition of Internal Auditing, the Code of Ethics, and the Standards must be recognized in the internal audit charter. The chief audit executive should discuss the Definition of Internal Auditing, the Code of Ethics, and the Standards with senior management and the board.
- 1110 – Organizational Independence - … The chief audit executive must confirm to the board, at least annually, the organizational independence of the internal audit activity.
- 1311 - Internal assessments must include: Ongoing reviews of the performance of the internal audit activity; and Periodic reviews performed through self-assessment or by other qualified individuals within the organization.
- 2010.A1 – The internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually. The input of senior management and the board must be considered in this process.
- 2110.A1 – The internal audit activity must evaluate the design, implementation, and effectiveness of the organization's ethics-related objectives, programs, and activities.
- 2310 – Identifying Information - Internal auditors must identify sufficient, reliable, relevant, and useful information to achieve the engagement's objectives.
- 2410.A2 – Internal auditors are encouraged to acknowledge satisfactory performance in engagement communications.
- Falling short of considering fraud, per the Standards:
  - 1210.A2 – Internal auditors must have sufficient knowledge to evaluate the risk of fraud …
  - 1220.A1 – Internal auditors must exercise due professional care by considering ... Probability of significant errors, fraud, or noncompliance;
  - 2060 – Reporting to Senior Management and the Board - The CAE must report periodically to senior management and the board … significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by senior management and the board.
  - 2120.A2 – The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.
  - 2210.A2 – Internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives.

- Lack of a consistent definition of controls:
  - 2201 – Planning Considerations - In planning the engagement, internal auditors must consider: …The adequacy and effectiveness of the activity's governance, risk management and control processes compared to a relevant framework or model;
  - 2210.A3 – Adequate criteria are needed to evaluate controls. Internal auditors must ascertain the extent to which management and/or the board has established adequate criteria to determine whether objectives and goals have been accomplished. If adequate, internal auditors must use such criteria in their evaluation. If inadequate, internal auditors must work with management and/or the board to develop appropriate evaluation criteria.
  - Control Processes - The policies, procedures, and activities that are part of a control framework, designed to ensure that risks are contained within the risk tolerances established by the risk management process.

1300 Quality Assurance and Improvement Program
• 1310 Quality Program Assessments. The internal audit activity must adopt a process to monitor and assess the overall effectiveness of the quality program (including both internal and external assessments).
• 1311 Internal assessments must include: Ongoing reviews of the performance of the internal audit activity; and Periodic reviews performed through self-assessment or by other qualified individuals within the organization.
• 1312 External assessments must be conducted at least once every five years by a qualified, independent reviewer or review team from outside the organization. The potential need for more frequent external assessments as well as the qualifications and independence of the external reviewer or review team, including any potential conflict of interest, must be discussed by the CAE with the Board. Such discussions must also consider the size, complexity and industry of the organization in relation to the experience of the reviewer or review team.
• 1320 The CAE must communicate the results of external assessments to the board.
• 1330 IA may report that their activities are "conducted in accordance with the Standards for the Professional Practice of Internal Auditing" only if assessments of the quality improvement program demonstrate that the IA activity is in compliance with the Standards.
• 1340 If full compliance with the Standards and/or the Code of Ethics is not achieved and noncompliance impacts the overall scope or operation of the internal audit activity, disclosure must be made to senior management and the board.

Larry@LHubbard.com