

# 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.

## 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.
- In Audit Reports:
  - Have final draft of audit report available at end of field work.
  - 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.

## 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.
- 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

## Management and Board Interview Points

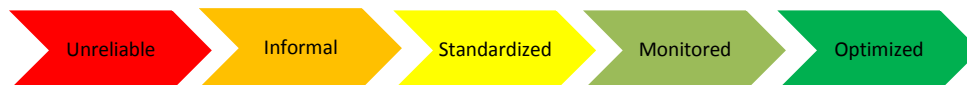
- Purpose of QAR
- Attitude and policies toward risks and controls
- Objectivity, credibility, effectiveness of IA activity
- Other comments about IA, controls, risks or governance.

## Audit Customer Surveys:

- |                                |                               |
|--------------------------------|-------------------------------|
| • Relationship with management | • Audit staff professionalism |
| • Scope of audit work          | • Audit process               |
| • Management of audit activity | • 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.





**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.

## New Release of IIA Standards

The release of the new *Standards* constitutes a milestone of the *Vision for the Future* task force recommendation to bring all authoritative guidance into the new International Professional Practice Framework (IPPF). The effective date of the comprehensive IPPF is January 2009.

1. Interpretations have been added to certain *Standards* to clarify terms or concepts. All interpretations are considered mandatory guidance and are integrated into each relevant standard. It is necessary to consider both the *Standards* and their interpretations to understand and apply the guidance correctly.

2. Six new *Standards* have been added:

**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.

**1111** - The chief audit executive must communicate and interact directly with the board.

**2110.A2** - The internal audit activity must assess whether the information technology governance of the organization sustains and supports the organization's strategies and objectives.

**2120.A2** - The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.

**2120.C3** - When assisting management in establishing or improving risk management processes, internal auditors must refrain from assuming any management responsibility by actually managing risks.

**2430** - Internal auditors may report that their engagements are conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing* only if the results of the quality assurance and improvement program support the statement.

3. Some amended wording of the current *Standards* has been introduced. Of particular significance is the replacement of **should** (which previously expressed a mandatory requirement) with **must**. This now occurs in most cases throughout the *Standards* to more clearly indicate unconditional requirements for properly conducting engagements. In five *Standards*, the word *should* is used to indicate engagement procedures that are usually expected to be undertaken. After considering them, a professional internal auditor but may determine that they are inappropriate, based on his or her knowledge and professional judgment.

4. New requirements in existing *Standards* (partial list):

- 1110 – CAE must confirm independence to board annually
- 1210.A2 – “IAs must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization” ... replaced identify “indicators of fraud.”
- 2010.A1 – Annual risk assessment must be documented
- 2060 – Periodic reporting to the Board now includes senior management, and fraud risks.
- 2230.A2 – Added “regardless of the medium in which each record is stored” to record retention.
- 2600 – Dropped “and senior management” from CAE discussion of unacceptable level of residual risks.

5. In most places, “irregularities” replaced with “fraud” and “record” replaced with “document.”

6. Modifications to existing terms within the Glossary have been added. It now includes definitions for *must*, risk appetite, *should*, etc.

## 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.