The Institute of Internal Auditors (IIA), USA- Quality Certification Requirements

Presentation by Vivek Sarabeswaran

2009

email: vivek@aptusconsultantsindia.com

Contents

Introduction on IIA's Quality Certification

1. The IIA, USA provides quality certification of internal audit departments by conducting External Quality Assessments (QA's)
2. A QA by IIA evaluates the internal audit activity for:
   - conformance with the International Standards for the Professional Practice of Internal Auditing (*Standards)*
   - the efficiency and effectiveness of the internal audit activity; and
   - the use of successful practices

3. The IIA has completed certifications for 283 companies world wide. Some of the reputed global organizations that have achieved IIA certification are Dell, Cummins, Kellogs, Microsoft, Shell, Siemens, Sun Microsystems, UNESCO etc.

4. The only Indian company to obtain QA certification from IIA is **"Ballarpur Industries"** in 2007.

Source: IIA website

Introduction on IIA's Quality Certification (continued...)

1. Validity of IIA certification – 5 years

2. Criteria for awarding QA certification – "General Compliance" with IIA Standards

3. **Recognition by IIA**

   - IIA will issue a **"plaque"** to the internal auditing activity (IAA) who gets an overall opinion of **"General Conformance"** in an external quality assessment conducted by IIA.

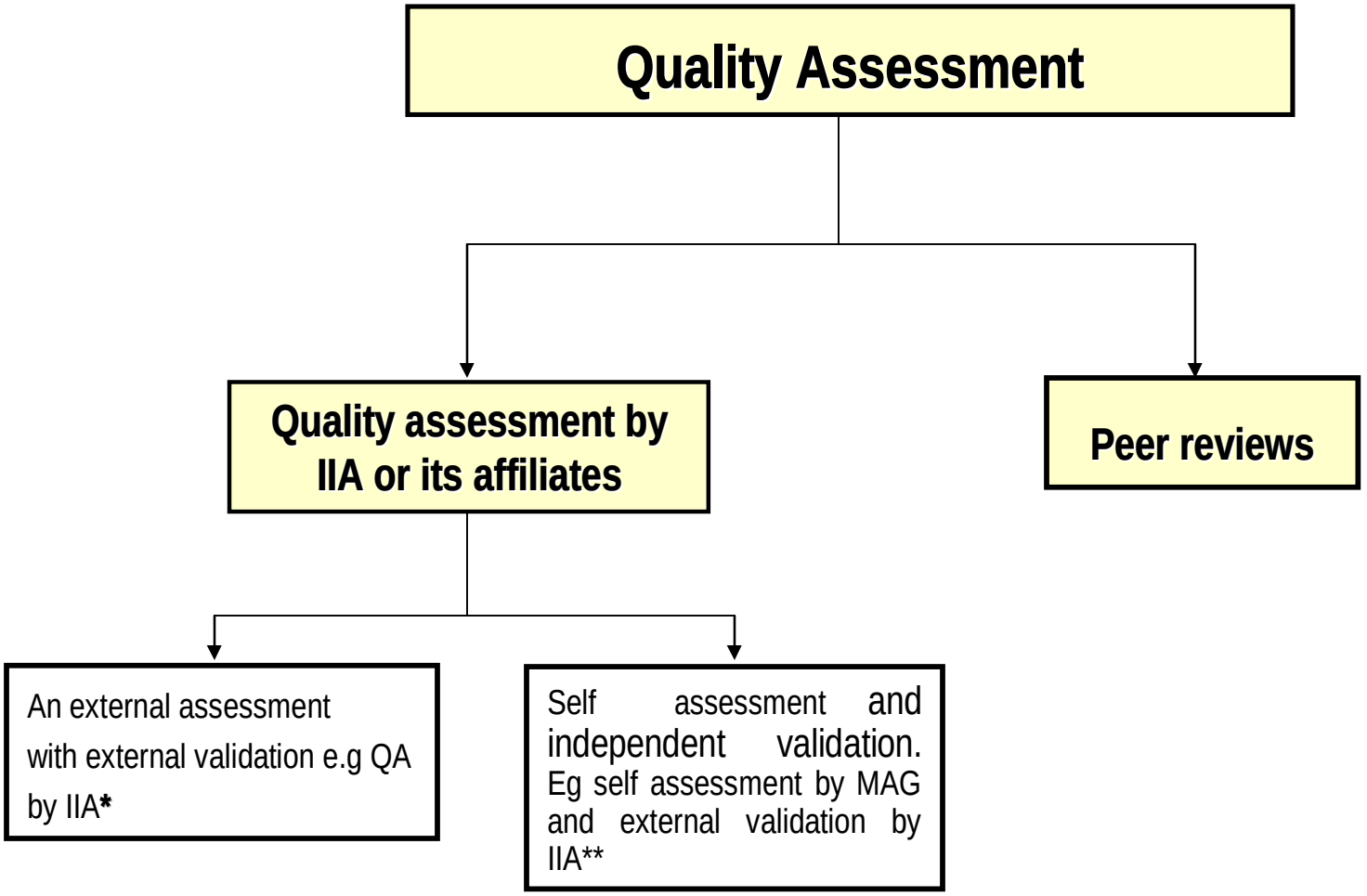
   - IIA will post the organization's name on its website for recognition.

4. On getting certification, audit reports can mention that "engagements are conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing"*

Benefits of IIA certification

- IIA certification is given to IA departments that follow **“best practices”** and have a relentless commitment to quality and in providing value addition to organization.
- External quality assessment reviews provide an **endorsement of the quality of the Internal Audit Department**
- Obtaining an external QA **provides evidence** to the board, management, and staff that the audit committee and the internal audit activity are concerned about the organization's internal controls, ethics, governance, and risk management processes
- It will measure the IAA to the current successful practices of the profession and **raise the profile of the IAA throughout the entire organization**.

Quality Assessment - Types



*** Recommended by IIA**

**** For small internal audit departments**

QA - Approaches

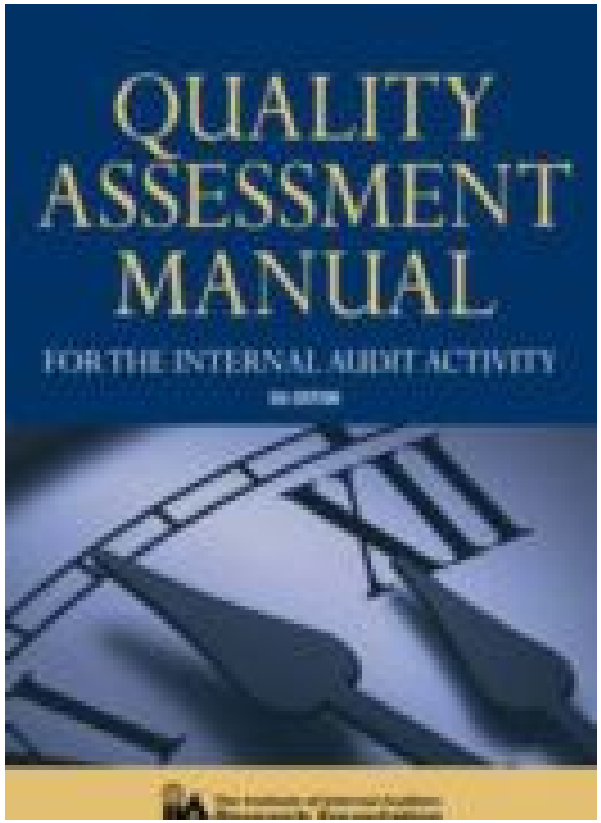
Full Independent review

- The IIA uses a **25% of audits** rule of thumb in a quality assessment with independent team review
- Each of the independent QA review team member would review *at least two sets of the working papers from the* ***current year and the year before.***

Self Assessment with Independent Validation (SAIV)

- The norm is to review 2-3 sets of work papers that were reviewed as part of the self assessment and then to review a couple that were not reviewed as part of the self assessment
- This is suitable for small internal audit departments

Tool used for QA



The Quality Assessment Manual (QAM), 6th Edition is the recommended toolkit for assessing compliance and will be used by IIA's review team for assessing compliance.

Compliance with IIA Standards & Code of Ethics

Definition of Internal Auditing

Definition of Internal Auditing

"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."

Assurance services

An objective examination of evidence for the purpose of providing an **independent assessment** on *risk management, control, or governance processes* for the organisation.

Consulting services

Advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and **improve** an organizations *governance, risk management, and control processes* without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation, and training.

Consulting services & Objectivity

Ensuring internal auditing maintains its objectivity

1. Internal auditors are not to assume management responsibilities, execute transactions or make ultimate decisions

2. Internal auditors should not audit their own work.

IIA Standards – Purpose

The **purpose** of the *Standards* is to:

1. Delineate basic principles that represent the practice of internal auditing.
2. Provide a framework for performing and promoting a broad range of value-added internal auditing.
3. Establish the basis for the evaluation of internal audit performance.
4. Foster improved organizational processes and operations.

The *Standards* are principles-focused, mandatory requirements consisting of:

- Statements of basic requirements for the professional practice of internal auditing and for evaluating the effectiveness of performance, which are internationally applicable at organizational and individual levels.
- Interpretations, which clarify terms or concepts within the Statements.

Classification of Standards

The Standards consists of three classifications:

Attribute standards – the **critical characteristics** that individuals, teams and organisations "**must have**" in order to provide effective internal audit services. Attribute standards cover issues such as:

- The purpose, authority, responsibility and charter of the Internal Audit activity
- Independence and objectivity
- Proficiency and due professional care
- Quality assurance and improvement

Attribute standards require full compliance.

Performance Standards – The description of the nature of internal audit services and **provide quality criteria** against which the performance of these services can be evaluated

Implementation Standards – More specific guidance as to how the Attribute and Performance Standards apply to each major type of internal audit activity. These augment the existing Attribute and Performance Standards by helping employ them in specific situations

Compliance – IIA's Standards & Code of Ethics

Overall Compliance Areas		
Attribute Standards (1000-1300)	**Performance Standards (2000 - 2600)**	**Code of Ethics**
1000 – Purpose, authority and responsibility 1100 - Independence and objectivity 1200 – Proficiency and due professional care 1300 – Quality assurance and improvement program	2000 – Managing the internal audit activity 2100 – Nature of work 2200 – Engagement planning 2300 – Performing the engagement 2400 – Communicating results 2500 – Monitoring progress 2600 – Management acceptance of risks	Principles and rules of conduct – ▪ Integrity ▪ Objectivity ▪ Confidentiality ▪ Competency
Implementation standards are included under the respective attribute or performance standards		

Categories of compliance

Each standard (Attribute, Performance and implementation) could have the following types of compliance

- **GC – "Generally Conforms"** means that the relevant structures, policies, and procedures of the 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"** means that the 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 falls short of achieving some major objectives.
- **DNC – "Does Not Conform"** means that the activity 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.
- **Key Conformance Criteria** – The Quality Assessment Manual includes Key Conformance criteria for each Standard and any of the Key Conformance Criteria not achieved, would strongly suggest a rating of "does not conform" or "partially conforms" for that individual standard

Standard 1000 – Purpose, Authority, and Responsibility

1000 – Purpose, Authority, and Responsibility - The purpose, authority, and responsibility of the internal audit activity must be formally defined in an internal audit charter, consistent with the Definition of Internal Auditing, the Code of Ethics, and the Standards. The chief audit executive must periodically review the internal audit charter and present it to senior management and the board for approval.

Key conformance criteria - A charter is a document that defines the mission, scope, responsibility, accountability, independence, authority and standard of audit practice. Essentially it is the guiding principles.

Standard 1010 – Internal Audit Charter

1010 – Recognition of the Definition of Internal Auditing, the Code of Ethics, and the *Standards* in the Internal Audit Charter

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.

Key conformance criteria - The charter includes reference to the Definition of Internal Auditing and the Code of Ethics consistent with the *Standards.*

Standard 1010 – Internal Audit Charter

Why are consulting services defined in the Internal Audit Charter?

The objective is to **retain independence and objectivity**. An example is **providing advice** on appropriate controls during IT system design phase with management having responsibility for accepting or rejecting the advice. Whereas if the auditor **led** the system design team and was responsible for implementation, the auditor's future ability to evaluate would be significantly impaired.

Some control measures for maintaining independence and objectivity are:

1. Charter language defining consulting service parameters
2. Policies and procedures limiting consulting projects
3. Segregation of consulting teams from assurance teams

Standard no.1110 – Organizational Independence

1110 - The chief audit executive must report to a level within the organization that allows the internal audit activity to fulfill its responsibilities. The chief audit executive **must confirm to the board, at least annually,** the organizational independence of the internal audit activity.

1110.A1 – The internal audit activity must be free from interference in determining the scope of internal auditing, performing work, and communicating results.

Key conformance criteria

1. The CAE reports to a level in the organization that is adequate to discharge his or her responsibilities.
2. Any reporting relationship (administrative or total) to management does not interfere with the CAE's responsibility to the board.
3. There are no restrictions to the scope, resources, and access of internal audit activity.

Standard 1111- Direct Interaction with the Board

1111 – Direct Interaction with the Board - The chief audit executive must communicate and interact directly with the board.

Key conformance criteria

No key conformance criteria. However examples of evidence, sound practices and other considerations would include interviews and Board minutes

Standard 1120 – Individual objectivity

1120 – Individual Objectivity - Internal auditors must have an impartial, unbiased attitude and avoid any conflict of interest.

Key conformance criteria

1. Auditors do not have assignments in conflict.
2. Audit staff has background and experience that does not conflict with audit assignment.
3. Results and conclusions of engagements are based on factual evidence and observation.

Standard 1130 – Impairment to independence or objectivity

1130 – **Impairment to Independence or Objectivity -** If independence or objectivity is impaired in fact or appearance, the details of the impairment must be disclosed to appropriate parties. The nature of the disclosure will be dependent upon the impairment.

1130.A1 – Internal auditors must refrain from assessing specific operations for which they were previously responsible. Objectivity is presumed to be impaired if an internal auditor provides assurance services for an activity for which the internal auditor had responsibility within the previous year.

1130.A2 – Assurance engagements for functions over which the chief audit executive has responsibility must be overseen by a party outside the internal audit activity.

1130.C1 – Internal auditors may provide consulting services relating to operations for which they had previous responsibilities.

1130.C2 – If internal auditors have potential impairments to independence or objectivity relating to proposed consulting services, disclosure must be made to the engagement client prior to accepting the engagement.

Key conformance criteria

1. Auditors are aware they must report any real or perceived conflict of interest as soon as such conflict arises.
2. Assignment of internal audit personnel takes into account previous responsibilities.
3. A policy exists to ensure that assurance engagements of areas which are under the control or direct influence of the CAE are overseen by a party external to the CAE.

Standard 1210 - Proficiency

Standard 1210 - Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.

1210.A1 – The chief audit executive must obtain competent advice and assistance if the internal auditors lack the knowledge, skills, or other competencies needed to perform all or part of the engagement.

1210.A2 – Internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.

1210.A3 – Internal auditors must have sufficient knowledge of key information technology risks and controls and available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.

1210.C1 – The chief audit executive must decline the consulting engagement or obtain competent advice and assistance if the internal auditors lack the knowledge, skills, or other competencies needed to perform all or part of the engagement.

Standard 1210 – Proficiency (continued…)

Key conformance criteria

1. Auditors undergo specific training based on collective staff training needs analysis.
2. Staff performance is reviewed on a regular basis and criterion used is adequate and appropriate for the needs of the activity. Where skills are lacking, CAE has engaged capable assistance.
3. Auditors have fraud training or proficiency in identification of fraud indicators.
4. Auditors have training or proficiency in IT concepts and computer aided audit tools. Where skills are lacking, the CAE has engaged capable assistance or has declined the engagement.

Standard 1220 – Due professional care

1220 – Due Professional Care - Internal auditors must apply the care and skill expected of a reasonably prudent and competent internal auditor. Due professional care does not imply infallibility.

1220.A1 – Internal auditors must exercise due professional care by considering the:

- Extent of work needed to achieve the engagement's objectives;
- Relative complexity, materiality, or significance of matters to which assurance procedures are applied;
- Adequacy and effectiveness of governance, risk management, and control processes;
- Probability of significant errors, fraud, or nonconformance; and
- Cost of assurance in relation to potential benefits

1220.A2 – In exercising due professional care the internal auditor must consider the use of technology-based audit and other data analysis techniques.

1220.A3 – Internal auditors must be alert to the significant risks that might affect objectives, operations, or resources. However, assurance procedures alone, even when performed with due professional care, do not guarantee that all significant risks will be identified.

1220.C1 – Internal auditors must exercise due professional care during a consulting engagement by considering the:

- Needs and expectations of clients, including the nature, timing, and communication of engagement results;
- Relative complexity and extent of work needed to achieve the engagement's objectives; and
- Cost of the consulting engagement in relation to potential benefits.

Standard 1220 – Due professional care (continued…)

Key conformance criteria

1. Audit workpapers provide evidence of due professional care in the conduct of the work performed.
2. Audit engagements are supported by **appropriate tools, including information systems** and used in an appropriate manner.
3. There is evidence of a **risk assessment** of the audit engagement.
4. Consulting engagement documentation provides evidence of due professional care in the conduct of the work performed.

Standard 1230 – Continuing Professional Development

1230 – Continuing Professional Development - Internal auditors must enhance their knowledge, skills, and other competencies through continuing professional development.

Key conformance criteria

There is continuing professional development to enhance the knowledge and competencies of internal auditors.

Standard 1300 &1310 – Quality Assurance & Improvement Program

1300 – Quality Assurance and Improvement Program - The chief audit executive must develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity.

1310 – Requirements of the Quality Assurance and Improvement Program - The quality assurance and improvement program must include both internal and external assessments.

Key conformance criteria

- The internal audit activity has a process to monitor and assess the overall effectiveness of the quality program.
- The quality assurance and improvement program must include both internal and external assessments.

Standard 1311– Internal Assessments

Standard no. 1311 –Internal assessments must include:

- Ongoing monitoring of the performance of the internal audit activity; and
- Periodic reviews performed through self-assessment or by other persons within the organization with sufficient knowledge of internal audit practices.

Key conformance criteria

- There is evidence of ongoing reviews of the performance of the internal audit activity.
- Periodic reviews were performed through self-assessment or by other persons within the organization, with knowledge of internal audit practices and the *Standards*.

Ongoing quality monitoring (IIA Implementation Standards requirements)

- Written **feedback from audit customers**, audit committee and other stakeholders
- Using **checklists** or internal audit automation that ensures that certain steps are performed.
- Following audit policies and procedure
- Use of **performance metrics;**

Standard 1311– Internal Assessments (continued…)

Periodic internal assessments

1. Assess compliance with Activity's Charter, the *Standards* and Code of Ethics
2. **Self assessment** with Quality assessment Manual as the guidance or tool. CAE questionnaires can also be used.
3. Benchmarking the internal audit performance metrics against other relevant best practices
4. These periodic internal assessments are recommended during years **where external assessment is not performed**

Standard 1312– External Assessments

1312 – External Assessments - External assessments must be conducted at least once every five years by a qualified, independent reviewer or review team from outside the organization. The chief audit executive must discuss with the board:

- The need for more frequent external assessments; and
- The qualifications and independence of the external reviewer or review team, including any potential conflict of interest.

Key conformance criteria

There is evidence of comprehensive external reviews by qualified, independent reviewers.

Standard 1321– Use of "Conforms with the *International Standards for the Professional Practice of Internal Auditing*"

1321 – Use of "Conforms with the *International Standards for the Professional Practice of Internal Auditing*" - The chief audit executive may state that the internal audit activity conforms with the *International Standards for the Professional Practice of Internal Auditing* only if the results of the quality assurance and improvement program support this statement.

Key conformance criteria

There is appropriate wording in audit reports.

Standard 1322– Disclosure of Nonconformance

1322 – Disclosure of Nonconformance - When nonconformance with the Definition of Internal Auditing, the Code of Ethics, or the *Standards* impacts the overall scope or operation of the internal audit activity, the chief audit executive must disclose the nonconformance and the impact to senior management and the board.

Key conformance criteria

There is appropriate wording in audit reports.

Compliance with IIA Performance Standards

Standard 2010 - Planning

2010 – **Planning -** The chief audit executive must establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization's goals.

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.

2010.C1 – The chief audit executive should consider accepting proposed consulting engagements based on the engagement's potential to improve management of risks, add value, and improve the organization's operations. Accepted engagements must be included in the plan.

Key conformance criteria

1. The CAE has established risk – based plans in consultation with the Board /Audit Committee and senior management
2. Where appropriate, consulting engagements are in the annual audit plan

Recommended:

1. The audit plan risk assessment should establish a link between the proposed audit topics and the operational, strategic risks and IT related risks
2. The audit plan risk assessment takes account of feedback received from operational managers
3. Formal opinion from Board and senior management. e.g final approval of annual audit plan

Standard 2020 – Communication & Approval

2020 – Communication and Approval - The chief audit executive must communicate the internal audit activity's plans and resource requirements, including significant interim changes, to senior management and the board for review and approval. The chief audit executive must also communicate the impact of resource limitations

Key conformance criteria

1. The CAE has communicated the internal audit activity's annual plans, including significant interim changes, to senior management and the board.
2. The CAE also has communicated to senior management and the board the impact of resource limitations.

Standard 2030 – Resource Management

Standard no.2030 – Resource Management - The chief audit executive must ensure that internal audit resources are appropriate, sufficient, and effectively deployed to achieve the approved plan.

Key conformance criteria

1. Staffing plans and financial budgets are determined from annual audit plans and activities of the internal audit department.
2. The internal audit activity is organized to ensure proper coverage of the organization's audit universe.

Standard 2040 – Policies and Procedures

Standard 2040 – Policies and Procedures - The chief audit executive must establish policies and procedures to guide the internal audit activity.

Key conformance criteria

There are appropriate policies and procedures and they are communicated to and understood by the staff of the internal audit activity

Policies and Procedures Manual

Contents

1. Internal audit policies and overview – Mission statement, charter, operating principles and policies etc
2. Planning and execution of engagements
3. Resources, staffing and development
4. Quality assurance
5. Administration – Time reports, record retention etc
6. Formats

Recommended by IIA

Essentials: *An Internal Audit Operations Manual* is a compilation of sample resources, documents, reference materials, and ideas that can be used in whole, in part, or customized as input to developing a new internal audit activity manual or updating an existing one. It also provides some model practices as guidance for internal audit practitioners.

Standard 2050 - Coordination

2050 – Coordination - The chief audit executive should share information and coordinate activities with other internal and external providers of assurance and consulting services to ensure proper coverage and minimize duplication of efforts.

Key conformance criteria

Internal audit work is coordinated with that of the external auditors and with internal providers of assurance and consulting services.

Recommended practices:

1. Reports on meetings between internal and external auditors
2. Follow-up by internal audit of the external auditors' recommendations
3. Internal and external auditors share information about the results of their work (**reciprocal exchanges** of reports, etc.)

Standard 2060 – Reporting to Senior Mgt & Board

2060 – Reporting to Senior Management and the Board - The chief audit executive must report periodically to senior management and the board on the internal audit activity's purpose, authority, responsibility, and performance relative to its plan. Reporting must also include significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by senior management and the board.

Key conformance criteria

There is evidence that CAE reports appropriately to the board and senior management on the internal audit activity purpose, authority, responsibility, and performance as well as significant fraud and other risks.

Standard 2110 - Governance

2110 – Governance - The internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:

Promoting appropriate **ethics and values** within the organization;

Ensuring effective organizational performance management and accountability;

Communicating risk and control information to appropriate areas of the organization; and

Coordinating the activities of and communicating information among the board, external and internal auditors, and management.

2110.A1 – The internal audit activity must **evaluate the design, implementation, and effectiveness of the organization's ethics-related objectives, programs, and activities**.

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.

2110.C1 – Consulting engagement objectives must be consistent with the overall values and goals of the organization.

Key conformance criteria

Internal audit activity assesses and makes appropriate recommendations for improving the governance process in its accomplishment of the objectives specified in the *Standards*.

Standard 2110 - Governance

Concept of Governance as described in the Practice Advisory 2130-1

"An organisation uses various legal forms, structures, strategies, and procedures to ensure that it:

- Complies with society's legal and regulatory rules
- Satisfies the generally accepted business norms, ethical precepts, and social expectations of society
- Provides overall benefits to society and enhances the interests of specific stakeholders in both the short-term and long term
- Reports fully and truthfully to its owners, regulators, other stakeholders, and general public to ensure accountability for its decisions, actions, conduct, and performance."

Auditing Values

1. Some kind of coverage of organisational values is recommended to be included in audit work.
2. For e.g **"Equal opportunity to all"**– Review all HR policies, procedures, appraisals to identify if there could potential for non-adherence to these values.
3. Another e.g. Auditing specific departments which are responsible for aspects like Health, Safety and Environment to see if values are practised.

Standard 2110 - Governance

Evaluating Ethics – related objectives, Programs and Activities

Major Components of an enhanced ethical climate:

1. A formal code of conduct
2. Frequent communications and demonstrations of ethical attitudes and behaviour
3. Easily accessible ways for people to confidentially report alleged violations
4. Regular surveys of employees, suppliers and customers to determine the ethical climate of the organisation
5. Regular reference and background checks as part of hiring procedures

Leading practices:

- Effectively communicating risk and control information to appropriate areas of the organization.
- The internal audit activity evaluates the design, implementation, and effectiveness of the organization's ethics-related objectives, programs, and activities.
- Auditing values and ethics programs

Standard 2120 – Risk Management

2120 – **Risk Management -** The internal audit activity must evaluate the effectiveness and contribute to the improvement of the risk management processes.

2120.A1 – The internal audit activity **must evaluate risk exposures** relating to the organization's governance, operations, and information systems regarding the:

- Reliability and integrity of financial and operational information;
- Effectiveness and efficiency of operations;
- Safeguarding of assets; and
- Conformance with laws, regulations, and contracts.

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

2120.C1 – During consulting engagements, internal auditors must address risk consistent with the engagement's objectives and be alert to the existence of other significant risks.

2120.C2 – Internal auditors must incorporate knowledge of risks gained from consulting engagements into their evaluation of the organization's risk management processes.

Standard 2120 – Risk Management (continued…)

Key conformance criteria

1. The scope of internal audit includes appropriate evaluation of risk management and control systems
2. Consulting projects cover all significant risk activities within the scope.
3. The potential for fraud and the organization's fraud risk has been addressed.

Best practices

.

1. Both enterprise-wide risk assessment and **preliminary specific engagement level risk assessment are to be done**
2. Definition of audit universe is important in risk assessment. Including components of the strategic plans of business units is important.
3. Risk assessment must consider inputs of senior management and Board.
4. Using some form of a Risk / Control Matrix in engagements is recommended.

Assessing Risk – Toolkit

This toolkit is published by the IIA Research Foundation

Contents

- Section 1 Overview: A description of the tool kit and an introduction to risk
- Section 2 Risk Assessment: The three-step process of assessing risk
- Section 3 Assessing Risk in Auditable Units: Performance Standard 2201
- Section 4 Building the Annual Audit Plan: Performance Standard 2010
- Section 5 Organizational Risk Assessment and Consulting Projects
- Section 6 Documenting and Reporting on Risk Assessment

Risk / Control Matrix

Business / Objective (1)	Risks (2)	Likelihood / Significance (3)	Controls or Risk Management Techniques (4)	Evaluation of adequacy (5)	Tests of effectiveness (6)	Final Evaluation (7)

1. Identify the business objectives through discussions with Management
2. Identify risks – Ask Management as to what events or circumstances could prevent them from achieving these objectives.
3. Rate each risk in terms of likelihood of occurrence and significance – Eg High, medium, low
4. Identify the controls / risk management techniques
5. Evaluate the adequacy of controls through analytical and professional judgement (Upto **50% of time is usually spent in this phase** as this phase generates maximum value added
6. Test the effectiveness of controls. Recommended 25-35% of time is devoted to testing
7. Arrive at the final opinion on adequacy and effectiveness of internal controls

Source: Implementation of Professional Standards, IIA

Steps in Macro Risk Assessment

Defining the audit universe

The audit universe is the sum of all auditable units. Auditable units are those parts of the organization that are exposed to sufficient risks that control, including audit, is appropriate.

Principles for defining audit universe

Risk identification

A thorough understanding of the business (for macro risk assessment) and a thorough understanding of the major business processes of the auditable unit (for micro risk assessment).

- Analogies to similar operations
- Prior history of the auditable unit
- Common sense or experience.
- Industry information

Risk Factors

The use of observable or measurable factors to substitute for measuring a specific risk or class of risks

Macro Risk Assessment– A simple example

RISK FACTORS RISK MEASUREMENT PROCESS

	FACTORS	F1	F2	F3	F4	F5	TOTAL
	WEIGHTS	**0.25**	**0.3**	**0.2**	**0.15**	**0.1**	**1.00**
AUDIT #	**AUDIT UNIVERSE**						
S102	Customer Billing	5	3	4	4	2	3.75
M102	PC/LAN Security	2	5	2	5	5	3.65
M101	Data Center Security	4	4	2	3	4	3.45
P301	T & E Expenses	3	3	2	4	5	3.15
A201	MRPII	2	5	1	4	2	3.00
P201	Payroll Time Reports	4	2	4	1	2	2.75
S101	Customer Contact	1	3	4	4	2	2.75
P101	Purchase Orders	5	1	3	1	3	2.60
S103	Sales Returns/Credits	3	2	2	2	5	2.55
P102	Contract Admin.	4	3	1	2	1	2.50
T101	Cashier Operations	3	1	2	3	5	2.40
P302	Misc. Dept. Expense	1	4	2	3	1	2.40
A102	Inventory Shrinkage	3	2	2	2	3	2.35
P202	Deduct/Remittances	2	1	3	1	4	1.95
F104	Depreciation	1	2	1	1	4	1.60

Risk Factors

F1 - Value in Rs.

F2 - Complexity

F3 - Volume of transactions

F4 - Mgt turnover

F5 - Time since last Audit

Micro / Process Risk Assessment– An example

WEIGHTED MATRICES RISK MEASUREMENT PROCESS													
Payroll Process EXAMPLE													
BUDGETED TESTING HOURS =					120								
.	S-T/Financial Matrix Wt =				0.65		Long term Matrix Wt =			0.35	Sum Matrix Wts =		1.00
FACTORS	F1	F2	F3	F4	F5		P1	P2	P3	P4	**TOTAL**		**TEST**
WEIGHTS	0.4	0.25	0.15	0.1	0.1		0.6	0.4	0	0	**SCORE**	**RANK**	**HOURS**
COMPONENTS													
Time reporting	4	5	3	4	3		2	6			3.86	4	21.47
Deductions and recoveries	5	6	6	4	3		5	2			4.65	3	25.84
Payroll software	3	7	4	6	5		3	7			4.63	2	25.77
Cheque printing & distribution	5	4	7	5	3		3	7			4.76	1	26.49
Account posting	3	4	7	5	5		1	5			3.67	5	20.43
										Total	**21.57**		**120**
Short term	**Long term**												
F1 - Errors	P1 - Training of employees												
F2 - Ommissions	P2 - High employee turnover												
F3 - Internal fraud													
F4- External fraud													
F5 - Level of automation													

Standard 2130 - Control

2130 – **Control -** The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.

2130.A1 – The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems regarding the:

- Reliability and integrity of financial and operational information;
- Effectiveness and efficiency of operations;
- Safeguarding of assets; and
- Compliance with laws, regulations, and contracts.

2130.A2 Internal auditors should ascertain the extent to which operating and program goals and objectives have been established and conform to those of the organization.

2130.A3 Internal auditors should review operations and programs to ascertain the extent to which results are consistent with established goals and objectives to determine whether operations and programs are being implemented or performed as intended.

2130.C1 During consulting engagements, internal auditors must address controls consistent with the engagement objectives and be alert to significant control issues.

2130.C2 Internal auditors must incorporate knowledge of controls gained from consulting engagements into evaluation of the organizations control processes.

Continued..

Standard 2130 - Control

Key conformance criteria

1. Where appropriate, audit work papers reflect the elements specified in the Implementation Standards.
2. Where appropriate, audit work papers reflect the elements specified in the Implementation Standards for consulting.

Standard 2201 – Planning considerations

2201 – Planning Considerations - In planning the engagement, internal auditors must consider:

- The objectives of the activity being reviewed and the means by which the activity controls its performance;
- The significant risks to the activity, its objectives, resources, and operations and the means by which the potential impact of risk is kept to an acceptable level;
- The adequacy and effectiveness of the activity's risk management and control processes compared to a relevant control framework or model; and
- The opportunities for making significant improvements to the activity's risk management and control processes.

2201.A1 – When planning an engagement for parties outside the organization, internal auditors must establish a written understanding with them about objectives, scope, respective responsibilities and other expectations, including restrictions on distribution of the results of the engagement and access to engagement records.

2201.C1 – Internal auditors must establish an understanding with consulting engagement clients about objectives, scope, respective responsibilities, and other client expectations. For significant engagements, this understanding must be documented.

Standard 2201 – Planning considerations (continued…)

Key conformance criteria

- Internal auditors systematically conduct a preliminary risk assessment of the organization's audit universe in order to **determine the engagement objectives**.
- Internal auditors develop and record a program for each engagement.
- In the case of outside engagements, the internal auditors establish a written understanding about the objectives, scope, and respective responsibilities of each party.

.

Standard 2210 – Engagement Objectives

Standard no.2210 – Engagement Objectives - Objectives **must be** established for each engagement.

2210.A1 – Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review. Engagement objectives must reflect the results of this assessment.

2210.A2 – Internal auditors must consider the **probability of significant errors, fraud, nonconformance, and other exposures when developing the engagement objectives**.

2210.C1 – Consulting engagement objectives must address governance, risk management, and control processes to the extent agreed upon with the client.

Engagement objectives can generally be summarised regarding the evaluation of

1. Reliability and integrity of information or recorded transactions.
2. Compliance with policies, directives, procedures, plans, laws, or regulations.
3. Safeguarding of assets.
4. Economic and efficient uses of resources.
5. Accomplishment of established goals and objectives for programs or operations.

Continued…

Standard 2210 – Engagement Objectives

Key conformance criteria

Internal auditors refer back to the preliminary risk assessment (Standard 2201) of the organization's audit universe in order to determine the engagement objectives.

Standard 2220 – Engagement Scope

Standard no.2220 – **Engagement Scope** - The established scope must be sufficient to satisfy the objectives of the engagement.

2220.A1 – The scope of the engagement must include consideration of relevant systems, records, personnel, and physical properties, including those under the control of third parties.

2220.A2 – If significant consulting opportunities arise during an assurance engagement, a specific written understanding as to the objectives, scope, respective responsibilities, and other expectations should be reached and the results of the consulting engagement communicated in accordance with consulting standards.

2220.C1 – In performing consulting engagements, internal auditors must ensure that the scope of the engagement is sufficient to address the agreed-upon objectives. If internal auditors develop reservations about the scope during the engagement, these reservations must be discussed with the client to determine whether to continue with the engagement.

Key conformance criteria

1. The engagement scope is consistent with the audit objectives.
2. If relevant, a written understanding and communication of consulting objectives, scope, and responsibilities.
3. There is evidence that results are communicated in accordance with consulting standards.

Standard 2230 – Engagement Resource Allocation

Standard no. 2230 – Engagement Resource Allocation - Internal auditors must determine appropriate and sufficient resources to achieve engagement objectives based on an evaluation of the nature and complexity of each engagement, time constraints, and available resources.

Key conformance criteria

There is evidence of appropriate evaluation of staffing after scoping that is based on nature and complexity of engagement, time constraints, and available resources**.**

Standard 2240 – Engagement Work Program

2240 – **Engagement Work Program -** Internal auditors must develop and document work programs that achieve the engagement objectives.

2240.A1 – Work programs must include the procedures for identifying, analyzing, evaluating, and documenting information during the engagement. The work program must be approved prior to its implementation, and any adjustments approved promptly.

2240.C1 – Work programs for consulting engagements may vary in form and content depending upon the nature of the engagement.

Key conformance criteria

1. The internal auditor has developed a formal engagement work program outlining the resources and procedures needed to achieve the audit objectives.
2. Fraud was considered in the program.
3. The engagement work program and subsequent program adjustments are approved in writing by the CAE or designee before the engagement is commenced.

Standard 2310 – Identifying Information

2310 – Identifying Information - Internal auditors must identify sufficient, reliable, relevant, and useful information to achieve the engagement's objectives.

Key conformance criteria

Workpapers include all the relevant information to achieve the objectives.

Standard 2320 – Analysis and Evaluation

2320 – Analysis and Evaluation - Internal auditors must base conclusions and engagement results on appropriate analyses and evaluations.

Key conformance criteria

Audit conclusions and engagement results are based on appropriate analyses and evaluations that identify the root cause(s) of irregularities**.**

Standard 2330 – Documenting Information

2330 – **Documenting Information -** Internal auditors must document relevant information to support the conclusions and engagement results.

2330.A1 – The chief audit executive must **control access** to engagement records. The chief audit executive must obtain the approval of senior management and/or legal counsel prior to releasing such records to external parties, as appropriate.

2330.A2 – The chief audit executive must **develop retention requirements** for engagement records, regardless of the medium in which each record is stored. These retention requirements must be consistent with the organization's guidelines and any pertinent regulatory or other requirements.

2330.C1 – The chief audit executive must **develop policies governing the custody and retention** of consulting engagement records, as well as their release to internal and external parties. These policies must be consistent with the organization's guidelines and any pertinent regulatory or other requirements.

Key conformance criteria

1. Sufficient information is documented to support the conclusions and audit results.
2. Workpapers have controlled access according to the policy of the organization
3. There is evidence that CAE obtains appropriate approvals prior to releasing records.
4. There is evidence of policy on retention requirements for assurance and consulting engagements.

Standard 2340 – Engagement Supervision

2340 – Engagement Supervision - Engagements must be properly supervised to ensure objectives are achieved, quality is assured, and staff is developed.

Key conformance criteria

There is evidence engagements are properly supervised as specified in the *Standards*.

Recommended:

1. Internal policies and procedures for the internal audit activity.
2. Approved engagement work program.

Standard 2410 – Criteria for communicating

Standard no. 2400 — Communicating Results - Internal auditors must communicate the engagement results.

Standard no.2410 – **Criteria for Communicating -** Communications must include the engagement's objectives and scope as well as applicable conclusions, recommendations, and action plans.

2410.A1 – Final communication of engagement results must, where appropriate, contain internal auditors' overall opinion and or conclusions.

2410.A2 – Internal auditors are encouraged to acknowledge satisfactory performance in engagement communications.

2410.A3 – When releasing engagement results to parties outside the organization, the communication must include limitations on distribution and use of the results**.**

2410.C1 – Communication of the progress and results of consulting engagements will vary in form and content depending upon the nature of the engagement and the needs of the client.

Key conformance criteria

1. There is evidence of appropriate, timely communication with management.
2. An overall opinion or conclusion is included in the audit report.
3. Satisfactory performance is acknowledged in engagement communications.
4. Communications outside the organization are limited in distribution and use of results.
5. There is evidence of progress and results on consulting engagements that is reasonable to the engagement.

Standard 2420 – Quality of Communications

2420 – Quality of Communications - Communications must be accurate, objective, clear, concise, constructive, complete, and timely.

Key conformance criteria

1. Communications are appropriate as stated in the *Standards*.
2. Audit reports are timely.

Standard 2421 – Errors and Omissions

2421 – **Errors and Omissions -** If a final communication contains a significant error or omission, the chief audit executive must communicate corrected information to all parties who received the original communication.

Key conformance criteria

Where appropriate, there is communication of corrected information to all parties.

Standard 2430 – Use of "Conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing*"

2430 – Use of "Conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing*" - 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.

Key conformance criteria

Use of "Conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing.*"

Standard 2431 – Engagement Disclosure of Nonconformance

Standard no. 2431 – **Engagement Disclosure of Nonconformance** - When nonconformance with the Definition of Internal Auditing, the Code of Ethics, or the *Standards* impacts a specific engagement, communication of the engagement results must disclose the:

- Principle or rule of conduct of the Code of Ethics or *Standard*(*s*) with which full conformance was not achieved;
- Reason(s) for nonconformance; and
- Impact of nonconformance on the engagement and the communicated engagement results.

Key conformance criteria

- Audit reports are distributed to an appropriate level of senior managers.
- If applicable, that the CAE properly considered the elements of the standard prior to disclosure outside the organization.
- Consulting engagement reports are distributed appropriately.

Standard 2440 – Disseminating Results

2440 – **Disseminating Results -** The chief audit executive must communicate results to the appropriate parties.

2440.A1 – The chief audit executive is responsible for communicating the final results to parties who can ensure that the results are given due consideration.

2440.A2 – If not otherwise mandated by legal, statutory, or regulatory requirements, prior to releasing results to parties outside the organization, the chief audit executive must:

Assess the potential risk to the organization;

Consult with senior management and/or legal counsel as appropriate; and

Control dissemination by restricting the use of the results.

2440.C1 – The chief audit executive is responsible for communicating the final results of consulting engagements to clients.

2440.C2 – During consulting engagements, governance, risk management, and control issues may be identified. Whenever these issues are significant to the organization, they must be communicated to senior management and the board.

Key conformance criteria

1. Audit reports are distributed to an appropriate level of senior managers.
2. If applicable, that the CAE properly considered the elements of the standard prior to disclosure outside the organization.
3. Consulting engagement reports are distributed appropriately.

Standard 2500 – Monitoring Progress

2500 – Monitoring Progress - The chief audit executive must establish and maintain a system to monitor the disposition of results communicated to management.

2500.A1 – The chief audit executive must establish a follow-up process to monitor and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action.

2500.C1 – The internal audit activity must monitor the disposition of results of consulting engagements to the extent agreed upon with the client.

Key conformance criteria

The CAE has established a follow-up process to monitor and ensure that management actions have been effectively implemented or risk accepted.

Standard 2600 – Management Acceptance of Risks

2600 Resolution of Senior Management's Acceptance of Risks - When the chief audit executive believes that senior management has accepted a level of residual risk that may be unacceptable to the organization, the chief audit executive must discuss the matter with senior management. If the decision regarding residual risk is not resolved, the chief audit executive must report the matter to the board for resolution.

Key conformance criteria

- Decisions regarding residual risk that are not resolved are reported by the CAE to the board for resolution.
- The subsequent resolution/disposition of such residual risk issues is appropriately documented.

Code of Ethics

The purpose of The Institute's Code of Ethics is to promote an ethical culture in the profession of internal auditing.

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.*

A code of ethics is necessary and appropriate for the profession of internal auditing, founded as it is on the trust placed in its objective assurance about governance, risk management, and control.

The Institute's Code of Ethics extends beyond the Definition of Internal Auditing to include two essential components:

1. Principles that are relevant to the profession and practice of internal auditing.
2. Rules of Conduct that describe behavior norms expected of internal auditors. These rules are an aid to interpreting the Principles into practical applications and are intended to guide the ethical conduct of internal auditors.

"Internal auditors" refers to Institute members, recipients of or candidates for IIA professional certifications, and those who perform internal audit services within the Definition of Internal Auditing.

Code of Ethics - Principles

Principles

Internal auditors are expected to apply and uphold the following principles:

1.Integrity

The integrity of internal auditors establishes trust and thus provides the basis for reliance on their judgment.

2.Objectivity

Internal auditors exhibit the highest level of professional objectivity in gathering, evaluating, and communicating information about the activity or process being examined. Internal auditors make a balanced assessment of all the relevant circumstances and are not unduly influenced by their own interests or by others in forming judgments

3.Confidentiality

Internal auditors respect the value and ownership of information they receive and do not disclose information without appropriate authority unless there is a legal or professional obligation to do so.

4.Competency

Internal auditors apply the knowledge, skills, and experience needed in the performance of internal audit services.

Code of Ethics – Rules of Conduct

Integrity

Internal auditors:

1. Shall perform their work with honesty, diligence, and responsibility.
2. Shall observe the law and make disclosures expected by the law and the profession.
3. Shall not knowingly be a party to any illegal activity, or engage in acts that are discreditable to the profession of internal auditing or to the organization.
4. Shall respect and contribute to the legitimate and ethical objectives of the organization.

Objectivity

Internal auditors:

1. Shall not participate in any activity or relationship that may impair or be presumed to impair their unbiased assessment. This participation includes those activities or relationships that may be in conflict with the interests of the organization.
2. Shall not accept anything that may impair or be presumed to impair their professional judgment.
3. Shall disclose all material facts known to them that, if not disclosed, may distort the reporting of activities under review.

Code of Ethics – Rules of Conduct

Confidentiality

Internal auditors:

1. Shall be prudent in the use and protection of information acquired in the course of their duties.
2. Shall not use information for any personal gain or in any manner that would be contrary to the law or detrimental to the legitimate and ethical objectives of the organization.

Competency

Internal auditors:

1. Shall engage only in those services for which they have the necessary knowledge, skills, and experience.
2. Shall perform internal audit services in accordance with the *International Standards for the Professional Practice of Internal Auditing.*
3. Shall continually improve their proficiency and the effectiveness and quality of their services.

Compliance Summary – Attribute Standards

PARTICULARS		(" " Evaluator's Decision)		
		GC	PC	DNC
OVERALL EVALUATION				
1000	**Purpose, Authority, and Responsibility**			
1010	Recognition of the Definition of Internal Auditing			
1100	**Independence and Objectivity**			
1110	Organizational Independence			
1111	Direct Interaction with the Board			
1120	Individual Objectivity			
1130	Impairments to Independence or Objectivity			
1200	**Proficiency and Due Professional Care**			
1210	Proficiency			
1220	Due Professional Care			
1230	Continuing Professional Development			
1300	**Quality Assurance and Improvement Program**			
1310	Requirements of the Quality Assurance and Improvement Program			
1311	Internal Assessments			
1312	External Assessments			
1320	Reporting on the Quality Assurance and Improvement Program (Not applicable for now)			
1321	Use of "Conforms with the *International Standards for the Professional Practice of Internal Auditing*" (Not applicable for now)			
1322	Disclosure of Nonconformance (Not applicable)			

Each standard (Attribute, Performance and implementation) could have the following types of compliance

- **GC – "Generally Conforms"** means the that the relevant structures, policies, and procedures of the 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"** means that the 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 falls short of achieving some major objectives.
- **DNC – "Does Not Conform"** means that the activity 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

Compliance Summary – Performance Standards

PARTICULARS		(" " Evaluator's Decision) GC	PC	DNC
OVERALL EVALUATION				
2000	**Managing the Internal Audit Activity**			
2010	Planning			
2020	Communication and Approval			
2030	Resource Management			
2040	Policies and Procedures			
2050	Coordination			
2060	Reporting to Senior Management and the Board			
2100	**Nature of Work**			
2110	Governance			
2120	Risk Management			
2130	Control			
2200	**Engagement Planning**			
2201	Planning Considerations			
2210	Engagement Objectives			
2220	Engagement Scope			
2230	Engagement Resource Allocation			
2240	Engagement Work Program			

PARTICULARS		(" " Evaluator's Decision) GC	PC	DNC
OVERALL EVALAUTION				
2300	**Performing the Engagement**			
2310	Identifying Information			
2320	Analysis and Evaluation			
2330	Documenting Information			
2340	Engagement Supervision			
2400	**Communicating Results**			
2410	Criteria for Communicating			
2420	Quality of Communications			
2421	Errors and Omissions			
2430	Use of "Conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing*"(Not applicable for now)			
2431	Engagement Disclosure of Nonconformance (Not applicable for now)			
2440	Disseminating Results			
2500	**Monitoring Progress**			
2600	**Management's Acceptance of Risks (Not applicable now)**			
IIA Code of Ethics				

Compliance Summary

		(“ ” Evaluator’s Decision)		
		GC	PC	DNC
Std.	**Contents**			
1000	Purpose, Authority, and Responsibility			
1100	Independence & Objectivity			
1200	Proficiency and Due Professional Care			
1300	Quality Assurance and Improvement Program			
2000	Managing the Internal Audit Activity			
2100	Nature of Work			
2200	Engagement Planning			
2300	Performing the Engagement			
2400	Communicating Results			
2500	Monitoring Progress			
2600	Management’s acceptance of Risks			
	Code of Ethics			
	Overall Evaluation			

Each standard (Attribute, Performance and implementation) could have the following types of compliance

- **GC – “Generally Conforms”** means the that the relevant structures, policies, and procedures of the 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”** means that the 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 falls short of achieving some major objectives.
- **DNC – “Does Not Conform”** means that the activity 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

Internal Auditing - Leading Practices

Observations from External Quality Assessments conducted by The IIA (Reproduced from IIA presentation)

Leading Practices

The IIA has conducted external quality assessments for over 18 years. Along with observations on *Standards* conformance, The IIA also has observed leading practices. Following is a brief list of some of The IIA QA Team observations of leading practices. Although not an exhaustive list, it does provide insights into what other IA activities are doing to make them "world class" in the profession of internal auditing.

Source: IIA website

Leading Practices - Risk Assessment and Audit Planning

The IA Activity seeks management's input to the Internal Audit risk assessment process, both as part of the annual audit planning and in the detailed audit planning for individual audits. **In planning individual audits, the IA Activity seeks management's input on both areas of risk and in suggestions for audit scope**.

Introduction of a new **"process auditing"** approach, coupled with integrated audit work teams, to improve the effectiveness and scope of audits and enhance Internal Audit's value as a business partner.

IA Activity brainstorming sessions, during the planning and reporting phases of audit engagements, strengthen the audit engagement planning and reporting processes.

Source: IIA website

Leading Practices - Governance

The CAE **meets one on one with senior executives on a monthly basis** to increase management's awareness about governance, risk assessment, internal audit and the value of a strong control environment.

The IA Activity **facilitated Enterprise Risk Management (ERM)** sessions with each line of business, assisting each of them in developing the basis for quarterly risk reports. Currently the business units are responsible for ERM self-evaluations each quarter.

Use of technology, including the Issue Manager tracking tool, enhances the efficiency of Internal Audit. Issue Manager is used to track recommendations from Internal Audit, external auditors, and the Financial Compliance Group Sarbanes-Oxley processes; these are accessed by the Audit Committee, management, and the groups making the recommendations.

Source: IIA website

Leading Practices - Quality Assurance and Improvement

The IA Activity has a **quality assurance and improvement program** that includes external quality assessment and both periodic and ongoing internal quality assessment. A variety of performance metrics are used to monitor performance and these measures are communicated to the Audit Committee.

The IA Activity has implemented **internal quality assurance activities** that involve post-engagement reviews of execution and documentation, internal reviews/external benchmarking of selected other internal audit processes, and an array of metrics for measuring internal audit's performance.

The IA Activity uses a **balanced scorecard** to periodically measure the IA Activity's performance. Results are tracked quarterly and reported to the Audit Committee.

The IA Activity uses **6-Sigma** in project development to assist in identifying process improvements in the internal auditing activity.

Source: IIA website

Leading Practices - Professional Development

The IA Activity participates regularly in professional organizations related to Internal Audit, also holding leadership positions from time to time. Additionally, the IA Activity personnel have participated as volunteers for external quality assessments through the peer review program in conjunction with The IIA. This has yielded a network of professional contacts that are used for new ideas and benchmarking purposes.

With regard to staff academic and professional qualifications, the IA Activity holds an impressive record that is better than many other IA activities in the profession. For example, 97% of the professional members of the IA Activity have a Bachelor degree, 35% a Master of Science degree and 32% a Master in Business Administration degree. The record of obtaining professional certification is remarkable, as 50% of the 34 auditors in the IA Activity have earned professional designations as CIA, CPA, CISA, CMA, CFE, CGA, etc.

The IA Activity has implemented **successful Short-Term and Long-Term Audit Rotation programs**.

Source: IIA website

Leading Practices - Value Added Services

The IA Activity provides **consulting services** to help management implement internal controls on the front end of projects. This help is so valued that management has recommended that the IA Activity staff be expanded to make more consulting resources available.

The IA Activity has developed a secure **Board of Director's web page** that is accessible by only directors and other authorized management personnel. The CAE posts quarterly reports to the web page **at least one week before the related AC meetings**, and AC members can access them from anywhere in the world to prepare for the AC meetings. This is an effective method to allow timely communication between the CAE and the AC.

Source: IIA website

Leading Practices - Improving Audit Efficiency

The IA Activity uses an **automated audit management information system** that includes automated work papers, issue tracking, time reporting, audit planning, personnel administration, and business risk profiles.

The IA Activity uses **audit software tools such as Audit Command Language** to increase staff efficiency and to allow for the review of large amounts of data and the selection of representative samples.

The **Database of Audit Findings**, which includes both internal and external findings, is considered important by both customer management and the IA Activity. The database is well maintained and the status of findings is updated regularly.

Source: IIA website

Leading Practices - Innovative Audit Approach

The IA Activity introduced a new "**process auditing**" approach, coupled with integrated audit work teams, to improve the effectiveness and scope of audits and enhance the IA Activity's value as a business partner.

The IA Activity identifies **"Red Action Items" and COSO control attributes** in audit reports, which is an effective means of communicating important issues and control considerations.

Source: IIA website

External Quality Assessments

Frequently Occurring Findings Observed by The IIA QA Teams (Reproduced from IIA's website)

Standard 1000

Observation

The IA Activity charter is **not updated** on an annual basis. The IA activity charter requires revision to consider The IIA's new definition of internal auditing, to reflect the CAE's responsibilities, and to obtain approval from the Audit Committee.

Recommendation

Update the IA activity audit charter on an annual basis to ensure it contains all the responsibilities of the IA Activity. Obtain the Audit Committees approval of the revised charter.

Source: IIA website

Standard 1110

Observation

The organization chart shows that the **CAE has a direct reporting relationship to the Executive Vice President and Chief Operating Officer** and a dotted line relationship to the Audit Committee.

Recommendation

The Audit Committee should evaluate the CAE reporting relationship to ensure the independence of the CAE is not impaired.

Source: IIA website

Standard 1210

Observation

There is a perception on the part of clients, based on the client survey results and management interviews, that the IA Activity Staff does not possess the desired level of business knowledge.

Recommendation

Increase auditor knowledge of business operations through staff rotation programs and in house training on business operations.

Source: IIA website

Standard 1210

Observation

The internal audit activity should possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities, including knowledge of key information technology risks and controls.

Recommendation

Enhance information technology audit coverage by hiring information technology audit specialists, providing additional specialized IA staff training and/or engaging IT audit contractors with appropriate qualifications.

Source: IIA website

Standard 1300

Observation

The IA Activity uses the *Standards* to generally define the Profession's audit quality, but has not set up a formalized quality assurance and improvement program, as called for In *Standard* 1300.

Recommendation

Establish and document a Quality Assurance and Improvement Program as set forth in the *Standards* and Practice Advisories.

Source: IIA website

Standard 1311

Observation

While several elements of the new *Standards* on quality assurance have been implemented by the IA Activity, the internal ongoing assessments could be strengthened by additional monitoring and benchmarking.

Recommendation

Implement an ongoing internal quality assessment process with the use of performance metrics (e.g., cycle time, customer satisfaction, cost recovery, balanced scorecard) which can be monitored on an ongoing basis.

Source: IIA website

Standard 2010

Observation

The IA Activity does not have a formal, documented risk assessment model for audit planning.

Recommendation

Formalize the annual audit planning and risk assessment process to more closely conform to IIA *Standard 2010.*

Source: IIA website

Standard 2010

Observation

While the audit universe has been identified, the annual audit plan does not include all entities in the audit universe.

Recommendation

Establish an internal audit risk assessment process to determine the priorities of the IA activity, consistent with the company's goals and objectives.

Source: IIA website

Standard 2030

Observation

The CAE should implement use of metrics to measure actual internal auditing performance against budget.

Recommendation

Use metrics to compare the actual use of resources to the budget.

Source: IIA website

Standard 2040

Observation

There is no formal internal audit policies and procedures manual governing the operating activities of the IA activity.

Recommendation

Develop an IA activity audit policies and procedures manual to help guide the operations of the audit Department.

Source: IIA website

Standard 2330

Observation

A set of working paper standards needs to be developed and formally defined in the IA activity policies and procedures. A review of working papers indicated the quality varied between audit staff.

Recommendation

Develop and enforce working paper standards, including sample formats, documentation requirements, indexing, and cross-referencing techniques with sufficient flexibility to serve as guidance for all types of audits, reviews, and evaluations.

Source: IIA website

Standard 2420

Observation

A review of work papers disclosed that the audit report for 80% were issued later than scheduled.

Recommendation

Improve the timeliness of audit reports by reducing the current time gap between the audit closing and the issuance of the report.

Source: IIA website

Standard 2420

Observation

Management interview comments indicate audit reports are not perceived as timely.

Recommendation

Shorten the time taken to issue audit reports.

Source: IIA website

Leading Practice

Observation

A formal program of career development and use of rotational employees has not been established and should be considered in the long-term.

Recommendation

Institute an employee rotation program that would provide opportunities for operating managers to gain experience across the company and also provide the IA Activity with a steady stream of fresh business knowledge for the audit staff.

Source: IIA website

Leading Practice

Observation

The company lacks a management control policy statement that clearly defines the responsibilities of the audit committee, senior management, and the IA Activity.

Recommendation

Consider implementing a management control policy that would provide a single statement on controlling the activities of the organization to clarify the control responsibilities of the Audit Committee, management and the IA activity.

Source: IIA website

Practice Advisory 2060.2

Observation

The charter does not call for Audit Committee participation in the selection or removal of the CAE, nor does the charter call for AC approval of annual compensation and salary treatment for the CAE.

Recommendation

Consider AC participating in the selection, removal and compensation of the Chief Audit Executive (CAE).

Source: IIA website

Practice Advisory 2060-2

Observation

The current Audit Committee Charter does not mention any role the Audit Committee may have in setting or approving the CAE's compensation.

Recommendation

Revise the Audit Committee Charter to require concurrence on the CAE's compensation and annual merit increase.

Source: IIA website