INTERNAL CONTROL STRUCTURE AND ASSESSMENT (ICA)

DEFINITIONS –

INTERNAL CONTROL – an activity, parameter, boundary or action taken by management to mitigate risk and exposure, while increasing the likelihood of achieving established objectives;

CONTROL ENVIRONMENT – often referred to as 'Tone at the Top', involves the setting created by upper management that involves; integrity, values, ethics, and a commitment to competence. It is reflected by the structure of the organization, including the reporting lines through hierarchy, the operational and functional definitions, and the philosophy and style of management;

INTERNAL CONTROL ASSESSMENT – an evaluation of the structure of Internal Control (as defined above), which is management's reaction to risk.

INTERNAL CONTROL QUESTIONNAIRE (ICQ) – a management self-reporting method using questions designed to provide information about the business process, function, or system being reviewed. The ICQ becomes the basis for the narrative and or flowchart of processes and their related internal controls, while an evaluation of the responses provided, guide the nature and extent of further tests of controls sufficient to perform the Internal Control Assessment. The questions are developed based on the Engagement Team's initial perception of the Business Objectives and the related risks (including fraud risks), existing policies and procedures, contracts, etc.

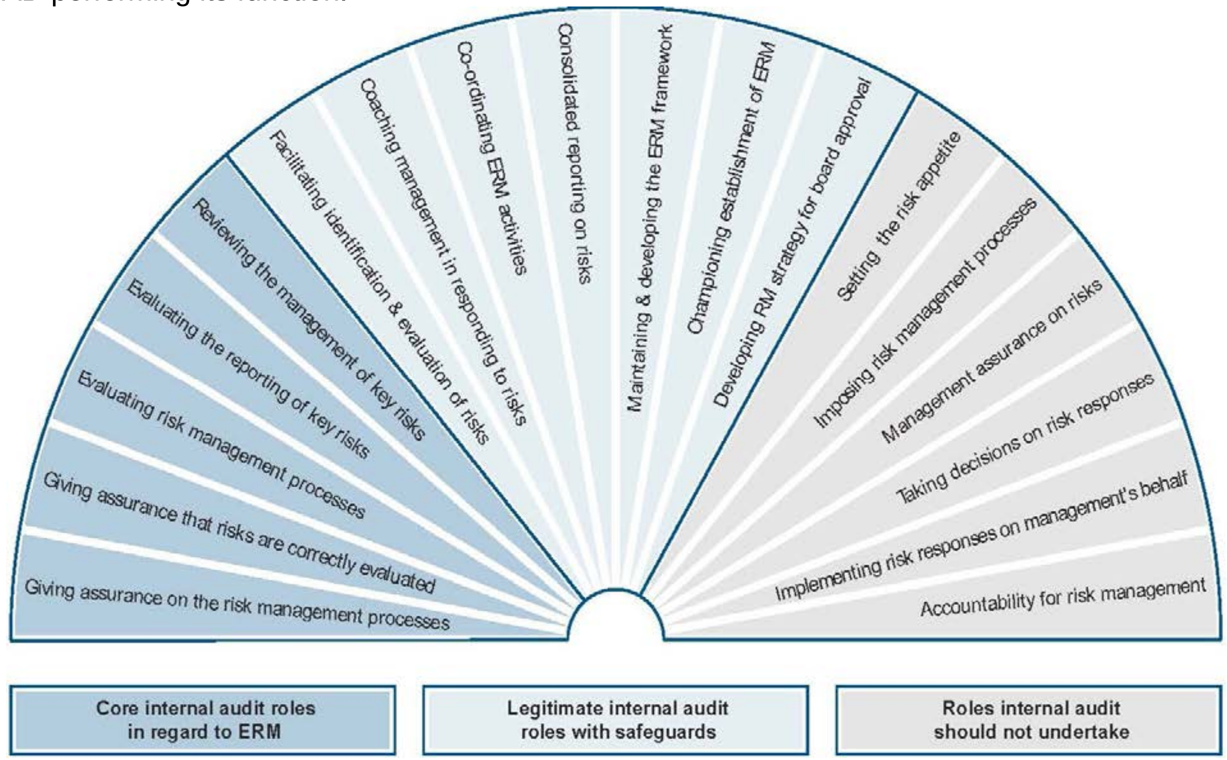
BACKGROUND –

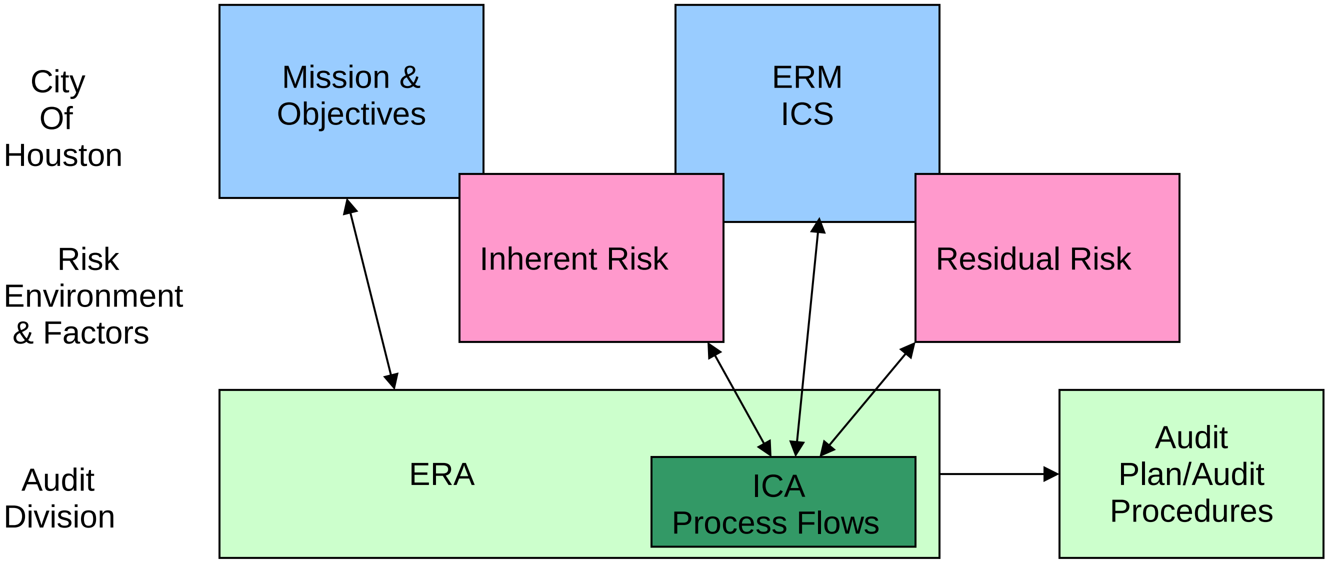
The Internal Control Structure (ICS) is based, in part, on environmental (business and physical), economic factors, political factors, and management's overall "appetite" for risk or its aversion. The ICS can be designed, created, and monitored using the Committee of Sponsoring Organizations for the Treadway Commission (COSO) framework of Internal Control and ERM. It is management's responsibility to develop this structure as it relates to the entity addressing risk through the creation and application of business, financial, operational, and information processes. This incorporates adequate systems of internal control, sometimes referred to as management control. In the broadest sense, "Internal Control" includes the environment, plans, policies, methods, and procedures adopted by management to meet its missions, goals, objectives and should be interwoven as an integrated function of its ERM.

The AD assumes responsibility to evaluate the adequacy/effectiveness and to make recommendations for the continual improvement of the risk management process. In order to maintain independence and objectivity, internal auditors must not develop the City's ICS; however, it is appropriate for the AD to act in a *consulting* capacity in some of these areas.

As should be clear at this point, internal controls are embedded and interactive with the risk management process and therefore, when looking at internal controls, they are inseparable because they were created to address risk. In fact, the result of the ICA provides information to support conclusions of the ERA and ARA, which then serves as a tool to plan, document, design, and perform subsequent procedures in adapting the specific audit/engagement objectives and audit/engagement program. The formality and depth of the ICA is based on the engagement, but it is always a consideration in planning and performing the necessary procedures to support conclusions.

The chart below is an excerpt from guidance issued by the IIA on ERM and Internal Audit's functional boundaries in relation to that process. The chart is mentioned here because the ICS is a key part of ERM. The boundaries outlined in the chart illustrate an important concept in the AD performing its function.


Giving assurance on the risk management processes
Giving assurance that risks are correctly evaluated
Evaluating risk management processes
Evaluating the reporting of key risks
Reviewing the management of key risks
Facilitating identification & evaluation of risks
Coaching management in responding to risks
Co-ordinating ERM activities
Consolidated reporting on risks
Maintaining & developing the ERM framework
Championing establishment of ERM
Developing RM strategy for board approval
Setting the risk appetite
Imposing risk management processes
Management assurance on risks
Taking decisions on risk responses
Implementing risk responses on management's behalf
Accountability for risk management
Core internal audit roles in regard to ERM
Legitimate internal audit roles with safeguards
Roles internal audit should not undertake



APPROACH AND METHODOLOGY –

Regardless of the level to which the ICA is performed, it is a documented process, and the resulting conclusions are to be included in audit/engagement workpapers. The overall result of the ICA provides support for refining the RA process to identify the residual or unmitigated risk. This process is separated into two major analytical components: *design* and *operation*, as explained below.

DESIGN

Internal Auditors will obtain an understanding of the internal controls that are significant within the context of audit/engagement objectives. Common methods of obtaining an understanding of internal controls include interviews, observations, inspection of documents and records, review of prior audit reports, and direct tests. The ICQ is one of the required workpapers for documenting an auditor's understanding of internal controls. While obtaining an understanding of program processes and related internal controls, auditors will also determine whether it is necessary to evaluate information system controls. Internal Auditors will obtain or prepare either a process narrative and/or a process flow diagram in which control points are be identified (See section below). The process of assessing the *adequacy* of the design of ICS requires the identification and sufficient understanding of the Control Environment that is significant to the engagement/audit objectives. Adequacy is reflected in the *design* is identified as sufficient to mitigate risks to an acceptable level within the context of the audit objectives, without having tested their existence. Further stated, a deficiency in design exists when (a) a control necessary to meet the control objective is missing or (b) an existing control is not properly designed so that, even if the control operates as designed, the control objective is not met.

OPERATION

ICAs are conducted to determine their *adequacy* and then to determine their *effectiveness*. In order to test the *effectiveness* of Internal Controls, internal auditors will also perform limited testing of each key internal control point identified in program processes (commonly known as a walk-through and usually takes the form of an attribute test). Assessing the Internal Control system for *adequacy* and *effectiveness* is crucial, because it directly relates to the mitigation of risk associated with the achievement of City and Departmental missions, goals and objectives. Assessing Internal Controls also leads to the determination of engagement/audit scope, objectives and methodology (procedures). As a result of ICA, auditors may modify the nature, timing, or extent of procedures.

In the case of performance audits, "an Internal Control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions to prevent, detect, or correct (1) impairments of effectiveness or efficiency of operations, (2) misstatements in financial or performance information, or (3) noncompliance with provisions of laws, regulations, contracts, or grant agreements on a timely basis" (See Yellow Book, Std. 6.21).

A deficiency in operation exists when a properly designed control does not operate as designed, or when the person performing the control does not possess the necessary authority or qualifications to perform the control effectively.

DOCUMENTING ICA

The workpaper should provide a conclusion(s) on the adequacy of the design, while a walk-through should provide support for the conclusion(s) related to the efficiency and effectiveness of the operation and application of the internal controls.

Control points and any findings that result from the ICA will be summarized on the ERD (See *220.30 Risk Management and Risk Assessment*).

NOTE: Below is a table based on COSO Framework for internal controls and ERM. For each element of the framework there are suggested sources of data to develop and prepare the ICA.

RISK AND INTERNAL CONTROL ASSESSMENT GUIDELINES

	COSO Framework Components		ERM Components
1	Control Environment	1	Internal Environment
		2	Objective Setting
		3	Event Identification
2	Risk Assessment	4	Risk Assessment
		5	Risk Response
3	Control Activities	6	Control Activities
4	Information and Communication	7	Information and Communication
5	Monitoring	8	Monitoring

1	***Control Environment***	
	COSO Framework Elements	**Possible Assessment Methods**
	Integrity and Ethical Values	
	Commitment to Competence	Job descriptions, resumes, retention of competent people, turnover rates/longevity, budget to provide for adequate resources;
	Elected Officials – Mayor, City Council, City Controller	City Council, IA reporting and accountability, governing body, checks and balances;
	Management Philosophy and Operating Style	Department meetings, interview management and others (e.g. receptiveness and openness);
	Organizational Structure	Organizational charts (e.g. Are they well designed and consistent with objectives? etc.);
	Assignment of Authority and Responsibility	Functions operating consistently with organizational chart, perform interviews, etc.;
	Human Resources Policies and Procedures	

2	***Risk Assessment***	
	COSO Framework Elements	**Possible Assessment Methods**
	City-Wide Objectives	City mission statement, policies and procedures, interviews;
	Process-Level Objectives	Policies and procedures, departmental SOPs, departmental missions goals & objectives, interviews, reviewing/documenting process flows;
	Risk Identification and Analysis	Audit Universe (Auditable Entities), interviews to determine engagement risk, identification of audit risk;
	Managing Change	Procedures for maintaining critical documentation and processes, etc.;

3	***Control Activities***	
	COSO Framework Elements	**Possible Assessment Methods**
	Policies and Procedures	Procedures for maintaining current APs, EOs, SOPs, Code of Ordinances, etc.;
	Security (Application and Network)	Security policies and procedures, access limited to only essential personnel, assigned rights, authority, responsibility, and job roles;
	Change Management	Application/Process/Infrastructure change procedures (assess control points), ensure appropriate segregation of duties in the application change process;
	Business Continuity	Assess disaster recovery plan, backup procedures, cross training;
	Outsourcing	Assess adequacy of contract terms and assignment of responsibility;

4	***Information and Communication***	
	COSO Framework Elements	**Possible Assessment Methods**
	Quality of Information	Sample test system data versus source documentation;
	Effectiveness of Communication	Dept./Division/Functional Meetings – notes/minutes;

5	***Monitoring***	
	COSO Framework Elements	**Possible Assessment Methods**
	On-going Monitoring	Existence of monitoring function, adequacy of monitoring procedures, documented results of monitoring activities;
	Separate Evaluation	Are monitoring procedures and results evaluated by independent parties;
	Reporting Deficiencies	Existence of monitoring reports, level to which reports are directed, documentation of the resolution of reported deficiencies;

Relevant Professional Standards and Guidance

GAGAS

Financial Audits	4.02 – 4.33
Performance Audits	2.10 – 2.11, 6.16 – 6.30, 6.61 – 6.66, 7.19 – 7.20
Attestation Engagements	5.01 – 5.32
Nonaudit Services	2.12 – 2.13, 3.45 – 3.55

IIA Standards

1210 – Proficiency
- 1210.A1
- 1210.A2
- 1210.A3

1220 – Due Professional Care
- 1220.A1

2060 – Reporting to Senior Management and the Board

2100 – Nature of Work

2130 – Control
- 2130.A1
- 2130.A2
- 2130.A3
- 2130.C1
- 2130.C2

2201 – Planning Considerations

2210 – Engagement Objectives
- 2210.A1
- 2210.A2
- 2210.A3
- 2210.C1

2440 – Communicating Results
- 2440.A1
- 2440.A2
- 2440.C1
- 2440.C2

GAGAS

Overall Supplemental Guidance	A.02
Internal Control	A.03 – A.06
Management's Role	A1.08

IIA Practice Advisories

2120-1 Assessing the Adequacy of Risk Management Processes
2130-1 Assessing the Adequacy of Control Processes

Change History

Chg #	Date	Section	Description/Reason