RISK MANAGEMENT AND RISK ASSESSMENT

DEFINITIONS –

RISK – The potential or likelihood that established objectives are not met or that the occurrence of adverse effects in attempts to achieve those objectives materializes (without the impact of a control structure).

RISK ASSESSMENT (RA) – an evaluation of identified and prioritized risks with reported management controls to achieve or sustain desired outcomes and protect resources and assets.

ENTERPRISE RISK MANAGEMENT (ERM) – Management's ongoing process to; identify business and performance objectives, identify threats (risk/impediments) to achieving those goals and determine strategies, design and implementation of controls, and utilization of resources to achieve those objectives. *This involves setting the tolerance for potentially adverse results and drives prioritization of design and implementation of management controls.*

ENTERPRISE RISK ASSESSMENT (ERA) – Identification and evaluation of; ***the City's*** exposure to adverse effects, based on mission and objectives, the environment and system of internal control set by management. The ERA is the responsibility of the AD which drives the audit plan and prioritizes the utilization of resources. This requires the AD to define entities/processes/functions that can be audited or reviewed. The population of entities/processes/functions that the AD identifies is referred to as the "Audit Universe".

ENTERPRISE RISK MANAGEMENT ASSESSMENT (ERMA) – Identification, evaluation and conclusion on management's process for identifying, reacting/addressing, controlling, communicating, and monitoring risk (the AD considers the first two elements during the ERA and is not currently reported separately).

AUDIT/ENGAGEMENT RISK ASSESSMENT (ARA) – Same as ERA, except at the engagement/project, or activity level. Identification and evaluation of risks (business, information technology, and fraud/waste/abuse) associated with the audit/engagement/review *that includes consideration and evaluation of management controls*.

AUDITOR RISK/DETECTION RISK (AR) – The possibility that engagement findings, conclusions, recommendations, or assurances are improper, incomplete, or not properly supported. Also, it is the risk that the scope and objectives reviewed/audited are inconsequential to the organization, thus misallocating audit resources.

CONTROL RISK – The result or residual risk (likelihood) of failure that management controls are not effectively or efficiently designed or implemented to sufficiently meet the mission and objectives of the organization and protecting City Assets. Evaluating the **CONTROL RISK** is the responsibility of the auditor by considering and assessing the entity, project, or activity's internal control structure (efficient design and effective implementation) and rendering a conclusion (this is essentially the output of the Internal Control Assessment).

INHERENT RISK – Susceptibility to failure intrinsic to the entity's business and environment.

RESIDUAL RISK - The potential or likelihood that established objectives are not met or the occurrence of adverse effects in attempts to achieve those objectives after considering the internal control structure and other mitigating factors or, that the consumption of City assets exceeds the value of the achieved objectives.

ENGAGEMENT RISK DOCUMENT (ERD) – A required and primary document (See Procedure 240.10) used to illustrate the linear progression from the development of Engagement Objectives, identification of Risks and the Internal Controls in place to mitigate risks, assignment of Risk Ranking related to the adequacy on Internal Controls, and the development of Audit/Engagement Program Steps.

NOTE: Risk related to Fraud is covered in the Fraud Procedure (Procedure No. 280.00 – Fraud Considerations) of this manual and risks related to Information Systems and Technology are currently addressed in Procedure No. 290.00 – Considerations of Information Technology.

PURPOSE – (from the AD perspective)

ENTERPRISE RISK ASSESSMENT –

- Provides a basis for the annual audit plan (*the Plan*), initial engagement objectives and directs the focus of the AD on areas that are relevant to regulatory, statutory, and reporting requirements in addition to effective and efficient performance.

AUDIT/ENGAGEMENT RISK ASSESSMENT –

- Ensures audit efficiency by re-evaluating risks throughout the project and revising the objectives, scope and resources as necessary. The audit/engagement risk incorporates determining Controls Risk and Residual Risk by performing substantive testing of the control structure sufficient to render conclusions and report to management and other stakeholders.

AUDITOR INDEPENDENCE –

- Ensures auditor independence at the conceptual framework involving the organization, the audit engagement and the individual auditor performance levels.

Consideration of risk at the City-wide, engagement and individual levels contribute to the continual improvement of the City's risk management process (including Fraud Considerations). In addition, evaluation of the design, implementation, and effectiveness of the City's ethics-related objectives, programs and/or activities key to enhancing our understanding of the impact of that governance related risk.

BACKGROUND –

The ERA can be performed using internal resources, external service providers or both. Between 1996 and 2004, the City outsourced the risk assessment process and was performing it approximately once every 5 years. Beginning in FY2009, the AD began performing this process/project using internal staff and committing to an annual process as required by International Professional Practices Framework issued by the IIA. The first ERA performed solely by the AD was completed in 2010 by developing the Quantitative form of analysis. Since 2010, and as part of the QA function, the AD has expanded the process by considering Qualitative factors as well.

While performing an ERA using internal resources has an opportunity cost associated with it, the benefits have exceeded those costs exponentially and synergistically. The AD has gained significant amount of institutional knowledge, has increased the awareness and connection of risk to resource allocation and focus, and has created business relationships internally and externally that creates visibility, transparency, accountability, availability.

APPROACH AND METHODOLOGY –

The AD Risk Assessment Processes focus on three primary perspectives:

CITY-WIDE/ENTERPRISE VIA THE ERA – Identifies and provides the foundation to develop the Annual Audit Plan and prioritizes resources to execute

SPECIFIC AUDIT/ENGAGEMENT VIA THE ARA– refines the objectives and scope for efficiency and effectiveness

AUDITOR – independence, competency, sufficient and appropriate evidence that impacts the reliability of the conclusions rendered by the AD. This is performed primarily at the engagement level.

Therefore, it should be noted that risk is considered throughout the entire process from *the Plan* development through the completion of individual projects performed.

ENTERPRISE RISK ASSESSMENT –

ERA is comprised of four major components summarized by considering Quantitative and Qualitative factors:

QUANTITATIVE ANALYSIS

1. Risk Assessment of the known Audit Universe

QUALITATIVE ANALYSIS

2. Input from the AD team and directives, special projects and other engagements as requested by the elected officials (Mayor, City Council) and other stakeholders (other City Departments, external audit considerations, etc.);

3. Significant/Notable structural, economic, legislative or environmental changes (including changes that affect the Audit Universe); and

4. Consideration of Information Systems

QUANTITATIVE ANALYSIS –

The Framework for the Quantitative Analysis was developed by the AD in 2009-2010. The process included:

- Identifying Risk Criterion (attributes or components of risk)
- Assigning a weight (in percentage) to each attribute identified, essentially ranking the significance
- Identifying auditable entities (departments, divisions, locations, functions, processes, accounts, etc.) based on management objectives and related inherent and associated risks
- Defining range of assessment value (e.g. 1-5, High, Medium, Low, etc.) for the overall process

- Calculating/Measuring each attribute relative to the auditable entities (areas) identified using data analysis and other relevant and reliable information
- Multiplying the raw attribute score times the associated weight to determine the overall attribute score
- Sum the total of the overall attribute scores for the auditable entity resulting in the Quantitative Component of the auditable area
- Repeat the process for each auditable area within each department
- Aggregate results by Department and Key Business Process

On an annual basis, the AD updates 3-6 departments per year to provide full coverage every 4-6 years using the following general procedures with participation from and information provided by City management:

- Updates the audit universe;
- Updates the missions, goals and objectives associated with the auditable areas which make up the audit universe;
- Determines the Risks related to the potential failure of achieving those stated goals and objectives (including fraud considerations); and
- Updates the Risk Assessment information and Issues a report accordingly.

The Risk Criterion/Attributes and related Weights are shown below:

	Risk Criteria	Definition	Weighting
1	Complexity of Operations	The risk related to the complicated nature of operations, the existence of diversified and/or decentralized operations, and the need for specialized skills. Considerations include the size of operations and the stability of processes, management and staff.	10 %
2	Council & Public Interest	The risk that adverse publicity, public concern and/or negative perception will damage public confidence in the City of Houston resulting in an erosion of the legitimacy of the City's mission, goals, and objectives. Considerations also include the possibility of improper actions by officials, management, and staff.	5 %
3	Financial Impact/Concerns	The risk that events such as disasters, changes in market conditions, failure of services, breakdown in internal controls or other events under or beyond management's control will result in decreased revenue, increased expenditures, or misleading financial reporting. Factors include materiality, cash handling, payroll, transaction volume, and the opportunity to commit and conceal fraud.	15 %
4	Human Resources Concerns	The risk that human resources at all levels are not available, inadequately trained, and/or do not possess the necessary minimum experience. Factors include the lack of succession planning and high levels of turnover.	10 %
5	Regulatory and/or Compliance Risk/Concerns	The risk that an entity fails to comply with laws or regulations at the federal, state, and local levels or the failure to comply with contractual obligations.	10 %
6	Technology Concerns	The risk that inadequate technological resources will hinder the ability to accomplish goals. Considerations include obsolescence, new regulations, or software threats.	10 %
7	Time Since Last Audit	The risk that certain high-risk areas within the City are not audited on a periodic basis.	5 %
8	Mission Criticality	The risk that functions critical to the overall mission of the City will fail.	10 %

9	Internal Control Consideration	The risk that key internal controls as presented by management are not valid responses to identified risks.	10 %
10	Legal Claims	The risk that legal claims and suits filed against City departments in connection with their core operations will adversely impact budgetary capacity.	5 %
11	Public and Employee Safety Concerns	The risk that measures do not exist to prevent safety hazards, serious injury, or death.	10 %

The result of the Quantitative Evaluation provides an insight to the unmitigated risk based on auditor judgment coupled with data analysis.

QUALITATIVE ANALYSIS –

The AD considers additional factors that are not quantified, but are reported as items considered in developing the audit plan.

INPUT AND REQUESTS

Input from the AD team and directives, special projects and other engagements as requested by the elected officials (Mayor, City Council) and other stakeholders (other City Departments, external audit considerations, etc.);

NOTABLE CHANGES

Applying the risk-based methodology as noted above in preparation of the FY2013 Annual Audit Plan, the Audit Division considers significant changes of events, operational and/or business processes, as well as changes in departmental leadership that have occurred since the last risk assessment update. These changes whether individually or collectively may have an effect on the way the City conducts business operationally and with resources that are available.

SIGNIFICANT/NOTABLE CHANGES SINCE LAST UPDATE

Major transactions, contracts, economic, legislative or environmental changes are documented in the report and considered. The primary source for this information is the City Council agenda and minutes, monitoring City Council sessions and reviewing the backup and Requests for Council Action (RCAs)

CHANGES TO THE RISK UNIVERSE

Changes to the Risk Universe are considered when for example: there are Departmental and/or management structure changes; functions/responsibilities/processes are added or eliminated; and consolidation or centralization occurs between Departments or city-wide.

CONSIDERATION OF SIGNIFICANT INFORMATION SYSTEMS

The Audit Division considers the City's information technology systems that have been implemented, as well as the technology initiatives that are being developed and acquired or updated. This includes, but not limited to: enterprise applications (financial, mail, security), major applications that interface or feed results/information into the ERP system, and systems that are primary and/or unique to a business model/department's operations, Infrastructure (WAN, LAN, Data Center(s), etc.)

From the results of the ERA, in conjunction with the identified Audit Universe, the AD recommends projects to be included in *the Plan*, which are approved by the CC.

AUDIT/ENGAGEMENT RISK ASSESSMENT (ARA)

Engagement Risk

The start of an ARA related to the activity under review is conducted during the planning phase. Risk is considered throughout the audit; however, with the implementation of the AD's planning process, changes to the initial ARA should be minimal and be related to unforeseen issues. The ARA is used to refine the ERA and to develop the initial scope and objectives of individual engagements identified in *the Plan*.

In performing the ARA, the AD considers the following:

1. Management's assessment of risks relevant to the activity under review, also:
    - The reliability of management's assessment of risk.
    - Management's process for monitoring, reporting, and resolving risk and control issues.
    - Management's reporting of events that exceed the limits of the organization's risk appetite and management's response to those reports.
    - Risks in related activities

2. Obtain or update background information about the activities to be reviewed to determine the impact on the engagement objectives and scope.

3. If appropriate, conduct a survey to become familiar with the activities, risks, and controls to identify areas for engagement emphasis, and to invite comments and suggestions from engagement clients.

4. Summarize the results from the reviews of management's assessment of risk, the background information, and any survey work. The summary includes:

    - Significant engagement issues and reasons for pursuing them in more depth.
    - Engagement objectives and procedures.
    - Methodologies to be used, such as technology-based audit and sampling techniques.
    - Potential critical control points, control deficiencies, and/or excess controls.
    - When applicable, reasons for not continuing the engagement or for significantly modifying engagement objectives.

(IIA Standard 2110)

OUTPUT

The AD uses the ERD (See Procedures 220.30; 220.40; 240.10) to provide centralized support for pertinent considerations addressed during the planning and engagement risk assessment process (**NOTE**: this includes reference to an assessment of internal controls related to the activity under review, fraud considerations, risk ranking, audit/engagement program steps, and initial findings.) ***The document is part of the workpapers and takes the form of a matrix prepared within the planning phase. Supporting documentation for the matrix is attached to the audit steps that are performed in the planning phase.***

The Output of the ERD includes:

- Identification of Process Risk
- Evaluation of related Management Controls
- Development of Fieldwork Audit/Engagement Procedures

AUDITOR RISK (ALSO REFERRED TO AS DETECTION RISK)

Audit Risk, as defined in the Yellow Book is the possibility that auditors' findings, conclusions, recommendations, or assurance may be improper or incomplete, as a result of factors such as evidence that is not sufficient and/or appropriate, an inadequate audit process, or intentional omissions or misleading information due to misrepresentation or fraud. Audit risk includes the risk that auditors will not detect a mistake, inconsistency, significant error, or fraud during an engagement. Audit risk is controllable by internal auditors and can be reduced through proper planning and adjustments to the audit methodology when necessary during audit fieldwork (See Yellow Book, Std. 8.16).

Through audit/engagement planning, preliminary survey, ARA, and the ICA, the AD designs its audit/engagement program to reduce the Audit Risk to an acceptable level. To illustrate, if through the planning and preliminary survey, it is discovered that the area being audited/reviewed is more complex or is heavily reliant on systems that are not understood, the audit/engagement team may decide to adjust their scope to better focus on a manageable sub-section than what was originally outlined (e.g. reducing the number of locations/departments/divisions to examine, etc.). The reaction to the increased Audit Risk due to the high complexity resulted in refining the focus to better manage the expanded risk that was identified.

RELEVANT PROFESSIONAL STANDARDS AND GUIDANCE

GAGAS

PERFORMANCE AUDITS	8.03-8.05; 8.08-8.09; 8.16; 8.30-8.35; 8.39-8.40

IIA STANDARDS (ANNUAL AUDIT PLAN)

2010 PLANNING
- 2010.A1
- 2010.C1

2120 RISK MANAGEMENT
- 2120.A1
- 2120.C3

2060 REPORTING TO SENIOR MANAGEMENT AND THE BOARD

IIA STANDARDS (ENGAGEMENT PLANNING)

2201 PLANNING CONSIDERATIONS
2210 ENGAGEMENT OBJECTIVES
- 2210.A1

IIA IMPLEMENTATION GUIDANCE

2010 PLANNING
2060 REPORTING TO SENIOR MANAGEMENT AND THE BOARD
2120 RISK MANAGEMENT

2201 PLANNING CONSIDERATIONS
2210 ENGAGEMENT OBJECTIVES

CHANGE HISTORY

Chg #	Date	Section	Description/Reason
1	3/31/2016	All	Made minor grammatical edits
2	7/1/2019	Relevant Professional Standards	Updated to reflect updates to Professional Standards
3	11/21/2022	Purpose	To include language regarding ethics evaluation.