ENTERPRISE RISK ASSESSMENT FY2026

OFFICE OF THE CITY CONTROLLER

CHRIS HOLLINS
CITY CONTROLLER

FY2027
Report #2027-01
August 31, 2026

CHRIS HOLLINS
City Controller

The Honorable John Whitmire, Mayor
City of Houston, Texas

SUBJECT: OFFICE OF THE CITY CONTROLLER FISCAL YEAR 2026 ENTERPRISE RISK ASSESSMENT

I am pleased to submit the Fiscal Year (FY) 2026 Enterprise Risk Assessment (ERA), conducted by the Audit Division within the Office of the City Controller.

The Division changed its method this year. Prior assessments evaluated one department at a time. The FY2026 ERA used a single city-wide survey instrument, applied one scoring model to every response, and facilitated workshops with twelve business areas. Twenty-five business areas were solicited and twenty-four participated. The result is 258 risks organized into five categories and 30 sub-categories, along with the City's first opportunity to see these risks comprehensively.

One caution on how to read this report: the risks were identified and rated by the business areas that own them. The Audit Division standardized the instrument, facilitated the sessions, and applied the scoring method consistently to every response, but did not independently test the mitigating activities reported or the controls described.

These results will inform the FY2027 Audit Plan, directing independent assurance toward the areas where exposure appears greatest and where coordinated, cross-departmental attention is most likely to strengthen governance, protect public resources, and sustain reliable service delivery to residents.

Respectfully submitted,

Chris Hollins
City Controller
City of Houston, Texas

xc: City Council Members
Dr. Cynthia Wilson, Chief of Staff, Mayor's Office
Department Directors
Aubrey Hooper, Chief Administrative Officer, Office of the City Controller
Jennifer Pierce, Deputy Director, Audit Division, Office of the City Controller

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The FY2026 Enterprise Risk Assessment (ERA) adopted a citywide method: one survey instrument, a common scoring model, and facilitated validation sessions for departments with complex operations or elevated exposure. Twenty-four of twenty-five business areas participated, twelve via workshops, producing 258 scored risks grouped into five categories and 30 sub-categories. The enterprise view reveals conditions that appear modest in a single department but material when they recur across many.

Operational risks total for 129, exactly half of the risk universe, with additional concentrations in Compliance (47), Financial (47), Strategic (23), and Health, Safety, and Environment (12). This profile indicates the City's principal FY2026 exposure is execution capacity. It's not uncertainty about goals, but the ability to achieve them with current people, systems, and assets.

Five enterprise themes summarize the conditions most likely to affect service delivery, governance, and fiscal stewardship (ordered by risk count):

- **Technology, reliability and cybersecurity (43 risks)**
  Aging and fragmented infrastructure is the single largest sub-category (26), accompanied by 11 cyber resilience and access protection risks and 6 AI/data governance risks. Departments are balancing modernization against growing service demand and early AI adoption.

- **Workforce capacity (38 risks)**
  Recruitment & retention (17), staffing coverage (15), succession planning (3), and training (3) were reported across nearly every business area, making workforce the most cross-departmental condition even if not the largest by count.

- **Governance, records, and public trust (33 risks)**
  Legal exposure, records retention, ethics safeguards (19), internal control and audit readiness (6), stakeholder confidence and public trust (8).

- **Operational execution and coordination (27 risks)**
  Process gaps, inconsistent procedures, and service bottlenecks (14); cross-department coordination and information sharing (8); fragmented reporting limiting visibility into performance, cost, and compliance (5). This theme is direct evidence of the operational concentration noted above.

- **Fiscal capacity under pressure (27 risks)**
  Revenue limitations and funding gaps (16) and rising labor, benefits, insurance, and project costs (11). These risks sit alongside 20 additional financial exposures in grant management, accounting integrity, and vendor cost.

Two sets of risks sit outside the five themes because each is better read against something else.

1. **Procurement (21 risks)**
   Enterprise-wide view reveals operational delays (11), financial vendor cost exposure (6), and contracting compliance (4). These are issues that are harder to see in single-department reviews and that warrant coordinated remediation.

2. **Asset Lifecycle (13 risks)**
   Aging facilities, fleet, equipment, and deferred maintenance align to capital planning decisions. Delays of these investments increase future costs and risks.

The risks in this assessment were identified and rated by the business areas that own them. The Audit Division (with the assistance of Ernst & Young LLC) designed and standardized the instrument, facilitated the validation sessions, and applied the scoring model consistently to every response, but did not independently test the conditions reported or the controls described. The ERA is a risk-based planning tool and is not an audit.

These results will inform the forthcoming Audit Plan, directing independent assurance toward the areas where exposure is greatest and where coordinated, cross-departmental attention is most likely to strengthen governance, protect public resources, and sustain reliable service delivery to residents.

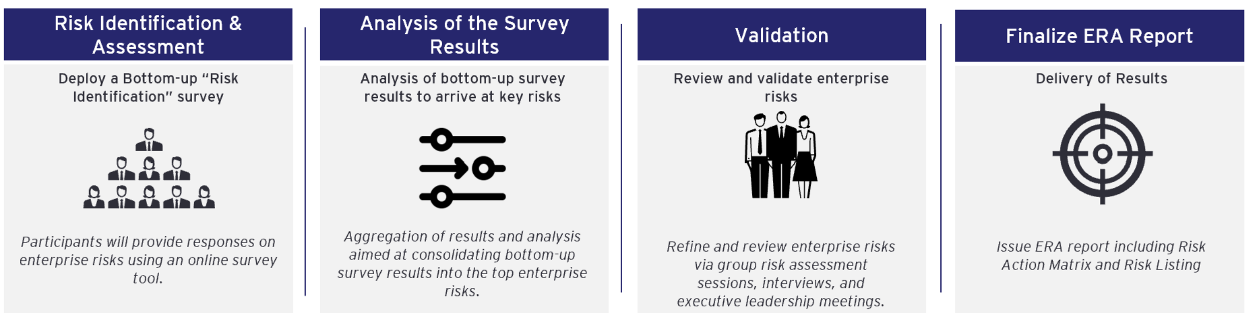
ENTERPRISE RISK ASSESSMENT

INTRODUCTION

The Audit Division follows GAGAS (Yellow Book) and the IIA Global Internal Audit Standards (Red Book), both of which require a risk-based approach to audit planning and execution. The Division applies this at two levels: an annual Enterprise Risk Assessment that identifies risks across the organization and informs the Audit Plan, and risk assessment at the engagement and process level within individual audits. Together these direct audit resources toward the areas of greatest potential impact.

BACKGROUND AND METHODOLOGY

The FY2026 City of Houston Enterprise Risk Assessment (ERA) was executed using a phased, stakeholder-driven approach designed to identify, validate, and prioritize enterprise risks aligned to the City's strategic objectives.



<u>RISK IDENTIFICATION AND ASSESSMENT</u>

The FY2026 ERA followed a structured, bottom-up approach beginning with Risk Identification & Assessment. A citywide "risk identification" survey was designed and deployed to leaders within each City business area to capture a broad view of enterprise risks. The survey was aligned to the City's risk taxonomy (e.g., strategic, operational, financial, compliance, and health, safety, & environment) and required respondents to define risks, describe impacts, and provide structured scoring inputs (likelihood, impact dimensions, and management preparedness). This approach generated a comprehensive, business area-level risk universe grounded in practitioner insight and enabled broad comparison across functions.

<u>ANALYSIS OF THE SURVEY RESULTS</u>

The second phase focused on aggregating and synthesizing survey inputs to identify the most significant and recurring risks across the City. Responses were consolidated and analyzed to identify common risk drivers, emerging patterns, and outliers, with outputs organized into an initial set of key risks. This bottom-up dataset was further enriched through external risk scans and benchmarking to provide context and challenge assumptions. The result was a refined, cross-departmental view of risks that served as the foundation for facilitated discussions and deeper validation.

VALIDATION

In the Validation phase, enterprise risks were reviewed and refined through targeted group risk assessment sessions, interviews, and executive discussions. Group sessions with operational stakeholders leveraged real-time collaboration tools to dynamically refine risk definitions, consolidate overlapping risks, and scored risks using the City-approved scoring model. Participants aligned on likelihood, impact, and preparedness to generate prioritized, department-level risk profiles. Follow-on interviews and leadership sessions focused on validating cross-cutting risks, confirming enterprise relevance, and resolving discrepancies resulting in a defensible, consensus-based enterprise risk profile.

Two disclosures apply to the validation phase. The Office of the City Controller participated as a business area alongside the departments it assesses; its responses were collected, scored, and validated using the same instrument and criteria applied to every other participant. The Audit Division and Ernst & Young LLC designed the assessment approach, facilitated the validation sessions, and is responsible for the analysis and conclusions presented in this report.

FINALIZE ERA REPORT

The final phase translated validated outputs into a comprehensive Enterprise Risk Assessment Report focused on identifying and consolidating risk themes that cut across the City of Houston. Individual risks were analyzed, normalized, and grouped into common enterprise-wide themes, enabling the identification of systemic challenges, shared root causes, and areas of concentrated risk exposure. The final ERA report provides leadership with a holistic view of the organization's most significant risk themes and will inform strategic decision-making, audit planning, risk mitigation priorities, and ongoing enterprise risk management efforts.

Risks were retained as submitted by each business area rather than deduplicated across business areas. Counts throughout this report therefore reflect the number of reported instances of a condition, not a count of independently validated distinct conditions, and a condition named differently by two departments appears twice

RISK SCORING

Each identified risk was evaluated using a standardized scoring methodology that assessed impact, likelihood, and management preparedness. Impact considered the potential consequences across compliance, financial, reputational, and service delivery dimensions, while likelihood reflected the probability of the risk occurring. Management preparedness evaluated the effectiveness and maturity of existing controls, mitigation strategies, policies, and governance mechanisms in managing the risk.

Participants assigned a rating of Low, Medium, or High for each criterion. Impact and likelihood scores were combined to determine the inherent risk rating, representing the level of risk in the absence of mitigating controls. The management preparedness assessment was then applied to evaluate how effectively the risk is currently being managed and to determine the residual risk rating, reflecting the level of exposure that remains after existing controls are considered.

This approach provided a consistent framework for comparing risks across departments and functions, enabling the City to prioritize risks based on both potential impact and organizational readiness. Additional information regarding the scoring methodology, rating criteria, and calculation approach is provided in Appendix 2.

RISK ANALYSIS

The FY2026 Enterprise Risk Assessment analyzed a broad set of 258 enterprise risks, identified through a combination of citywide survey responses and facilitated group risk assessment sessions, capturing perspectives from business area leadership across the City. As described in the assessment methodology, risks were defined, scored, and refined using standardized criteria for impact, likelihood, and management preparedness, resulting in a consolidated and prioritized enterprise risk profile. The resulting risk universe reflects a diverse mix of strategic, operational, financial, compliance, and external risks, with notable concentrations in areas impacting service delivery, workforce capacity, infrastructure, financial sustainability, and governance. Collectively, these risks highlight both cross-cutting challenges affecting multiple departments and function-specific pressures that may require targeted mitigation strategies.

The risk universe represents the full population of risk categories and related risk names that define the City's enterprise-wide risk landscape. Additionally, the risk universe provides a structured and consistent foundation for identifying and organizing risks that could affect the City's ability to achieve its objectives.

This year's risk universe will serve as the foundation for evaluating risk exposure across the City and identifying areas that may warrant additional review, monitoring, or audit attention. By organizing risks into consistent categories and sub-categories and applying standardized scoring criteria, the City Controller's office can compare risks across business areas, prioritize those with the greatest residual exposure, and align future audit planning with the risks most likely to affect service delivery, financial stewardship, compliance, operational resilience, and public trust. The complete list of identified risks is provided in Appendix 1.

RECURRING RISK TRENDS ACROSS THE ENTERPRISE

Analysis of survey results and group session inputs identified several risks that appeared consistently across the City. The recurrence of these risks suggests they are not isolated to individual functions but instead reflect systemic challenges affecting multiple departments where the City is experiencing consistent exposure. This pattern indicates emerging trends within the City's risk environment that may warrant coordinated, citywide attention and response.

The most frequently reported risks across the City of Houston indicate a consistent pattern of workforce, operational, infrastructure, and compliance challenges affecting multiple departments. Workforce-related risks emerged as some of the most pervasive concerns, highlighting ongoing difficulties in attracting, developing, and retaining the personnel needed to sustain service delivery. Operational challenges were also widely reported, particularly cross-departmental coordination and delayed procurement, which may hinder project execution and the timely acquisition of critical goods and services. Aged and inadequate facilities were another prominent concern, reflecting the growing burden of maintaining physical infrastructure and ensuring facilities can support evolving operational needs.

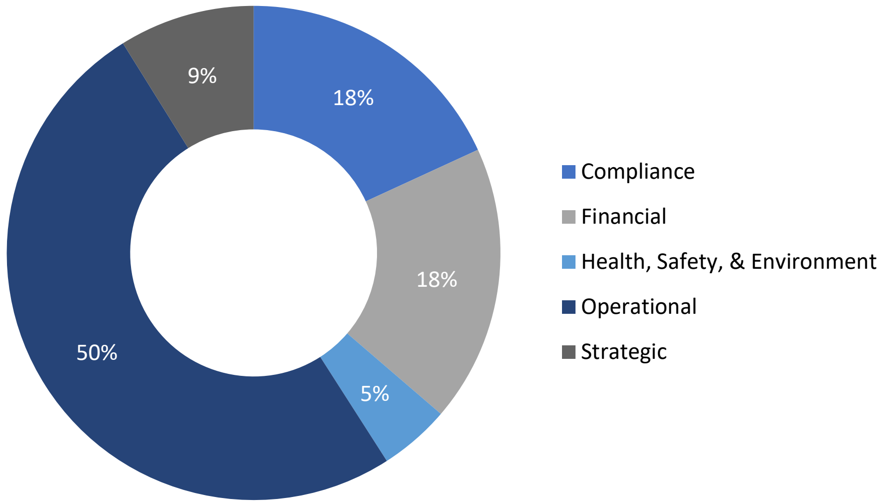
In addition, departments commonly identified risks related to records retention and cyber-attacks, underscoring the importance of strong governance, information management, and cybersecurity practices. Financial and regulatory pressures also emerged as recurring themes, including rising labor and benefits costs, grant funding shortfalls, changing regulatory landscape, regulatory compliance complexity, cost overruns, and insufficient budget allocations. Technology modernization challenges, particularly aging and fragmented technology infrastructure, further suggest that departments are balancing growing service demands with the need to update legacy systems. Collectively, these findings suggest that many of Houston's key risks are enterprise-wide in nature and will require coordinated, cross-departmental strategies to strengthen organizational resilience, maintain service levels, and support the City's long-term strategic objectives.

- Workforce Attraction and Retention
- Delayed Procurement
- Staffing Shortages
- Aged/Inadequate Facilities
- Records Retention
- Cyber Attack
- Changing Regulatory Landscape
- Regulatory Compliance Complexity
- Grant Funding Shortfalls
- Fraud, Waste, and Abuse
- Cross-Departmental Coordination
- Insufficient Budget Allocation
- Cost Overruns
- Aging/Fragmented Technology Infrastructure
- Rising Labor and Benefit Costs
- Workplace Safety
- HR Service Delivery
- Innovation and Modernization Pace
- Inventory Reporting

RISK CATEGORIZATION

Risk categorization provides the foundation for organizing and analyzing the results of the Enterprise Risk Assessment by grouping individual risks into a structured, consistent framework. At the highest level, risks are classified into broad categories (e.g., Operational, Strategic, Financial, Compliance, and Health, Safety & Environment).

City of Houston Risk Category Distribution



Sub-categories add a layer of precision beneath the five broad risk categories, grouping risks by how they manifest, such as technology reliability, funding stability, or workforce leadership. They were developed by identifying recurring themes in the risk names, descriptions, and impacts submitted across all responses, then organizing those themes into consistent groupings grounded in how risks appear in the data. The results support aggregation of common themes across departments and enable more targeted prioritization and response planning. The table below sets out each sub-category, its description, and the number of risks identified within it.

Risk Sub-Category	Sub-Category Description	# of Risks
COMPLIANCE (47 RISKS)		
AI & Data Governance	Oversight of artificial intelligence use, data privacy, access management, and responsible adoption across City operations.	6
Controls & Audit	Design, monitoring, and documentation of internal controls to support accountability, audit readiness, and risk mitigation.	6
Grant Compliance	Compliance with grant requirements, documentation standards, reimbursement conditions, and disaster recovery obligations.	5
Legal, Records & Ethics	Management of legal exposure, records obligations, ethics safeguards, and practices that support integrity and public trust.	19
Procurement & Contracting Compliance	Adherence to procurement and contracting requirements, including legal, policy, transparency, and approval standards.	4
Regulatory & Policy	Impacts from changes in laws, policies, and regulatory expectations affecting compliance, operations, and service delivery.	7
FINANCIAL (47 RISKS)		
Cost Inflation & Budget Pressure	Budgetary pressure is associated with rising labor, materials, insurance, overtime, and project costs.	11
Financial Accounting Integrity	Reliability, accuracy, transparency, and control of financial records, cash handling, expenditures, and reporting processes.	6
Grant Management	Oversight of grant funding, expenditures, reimbursements, and fiscal stewardship across complex programs.	8
Procurement Vendor Cost Exposure	Cost exposure is associated with vendor pricing, contract consolidation, maintenance support, and supply constraints.	6
Revenue Pressure and Budget Capacity	Revenue limitations, budget imbalances, and funding gaps that may constrain services, programs, and infrastructure investment.	16
HEALTH, SAFETY AND ENVIRONMENT (12 RISKS)		

Risk Sub-Category	Sub-Category Description	# of Risks
Animal Welfare & Zoonotic Risk	Risks related to animal care, shelter operations, zoonotic disease controls, and public confidence in animal welfare services.	3
Public Health and Emergency Readiness	Public health capacity, emergency preparedness, medical access, and incident response readiness.	3
Workplace Safety, PPE Preparedness	Employee safety, personal protective equipment readiness, workplace security, and continuity during hazardous conditions.	6
OPERATIONAL (129 RISKS)		
Coordination and Communication	Effectiveness of information sharing, cross-department coordination, and aligned planning needed to execute work efficiently.	8
Critical Asset and Infrastructure Lifecycle	Lifecycle management of aging facilities, fleet, equipment, infrastructure, and deferred maintenance needs.	13
Cyber Resilience and Access Protection	Cybersecurity, access controls, system resilience, and protection of critical information technology and operational technology assets.	11
Lack of Centralized Reporting	Fragmented data, reporting, and monitoring that limit visibility into performance, costs, inventory, and compliance.	5
Operational Process	Process gaps, inconsistent procedures, service bottlenecks, and operational practices that may reduce efficiency and effectiveness.	14
Procurement Delays	Delays in purchasing, contracting, approvals, and payment workflows that may affect projects and service delivery.	11
Staffing Capacity and Service Coverage	Staffing shortages, coverage gaps, workload pressures, and service demand that may affect operational capacity.	15
Succession Planning	Leadership continuity, knowledge transfer, and readiness to fill critical roles without disrupting operations or services.	3
Technology Reliability and Modernization	Reliability, modernization, integration, digital service quality, and performance of technology-enabled workflows.	26
Vendor Service Delivery	Vendor performance, third-party compliance, service quality, and reliability of outsourced operational support.	3
Workforce Recruitment and Retention	Ability to attract, engage, and retain critical talent amid labor market competition and compensation pressures.	17
Workforce Training	Training, coaching, knowledge development, and capability building needed to sustain effective workforce performance.	3
STRATEGIC (23 RISKS)		
External Disruption and Economic Shifts	Economic, climate, pandemic, geopolitical, and market disruptions that may affect priorities and operating conditions.	4
Intergovernmental Coordination and Policy Constraints	Intergovernmental dependencies, policy constraints, and coordination challenges that may limit local execution.	6
Public Trust, Stakeholder Confidence	Transparency, communication, reputation, and stakeholder engagement considerations that may affect confidence in City actions.	8
Strategic Goal and Priority Alignment	Alignment of goals, priorities, performance measures, and service strategies needed to achieve measurable results.	5

CONCLUSION

The FY2026 Enterprise Risk Assessment gives the City one comparable view of the risks most likely to affect service delivery, financial stewardship, compliance, operational resilience, and public trust. Exposure concentrates in five areas: technology reliability and cybersecurity, workforce capacity, governance and public trust, operational execution and coordination, and fiscal capacity. None of them stands alone. Limited funding and staffing delay technology refresh, which weakens cybersecurity posture. The same constraints extend deferred maintenance and slow procurement. Each pressure makes the next one harder to relieve, and together they strain the City's ability to sustain core services.

The assessment also identified several recurring risk themes that may not always rank among the highest residual scores, but still warrant audit consideration because of their frequency, cross-departmental nature, and potential to compound over time. Workforce attraction, retention, succession planning, and training appeared across multiple business areas and may affect continuity, institutional knowledge, and the City's ability to execute critical functions. Similarly, procurement delays, fragmented reporting, records retention, grant compliance, technology reliability, aging facilities, and public trust concerns reflect systemic challenges that may create control gaps, reduce transparency, or limit timely decision-making even when individual risks appear moderate in isolation.

Together, the highest-rated risks and the most common recurring themes should inform development of the Audit Plan by helping the Audit Division balance depth and breadth. High residual risks should be considered for targeted audits, advisory projects, or focused control reviews where exposure and preparedness gaps are greatest. Recurring risks should be considered for enterprise-wide or cross-cutting audit approaches that evaluate whether common root causes, such as decentralized ownership, limited data visibility, inconsistent procedures, or resource constraints, are affecting multiple departments. This dual lens helps ensure the Audit Plan addresses both urgent, high-impact risks and broader themes that may signal systemic exposure.

Overall, the ERA should serve as a practical bridge between enterprise risk identification and risk-based audit planning. By using the assessment to prioritize areas of high residual exposure, recognize recurring enterprise themes, and track how risks evolve over time, the Audit Division can focus audit resources on areas where independent assurance, control evaluation, and actionable recommendations are most likely to strengthen governance, improve operations, protect public resources, and support the City's ability to deliver reliable services to residents.

AUDIT TEAM

Ernst & Young, LLP
Deputy Director: Jennifer Pierce
Audit Manager: Theresa Watson, CIA, CGAP
Lead Auditor: Jermaine Brooks

APPENDIX 1: RISK UNIVERSE

The following appendix presents the complete enterprise risk inventory identified through the current-year assessment. Risks are organized by primary category and sub-category to support transparency, traceability, and alignment with risk-based audit planning.

COMPLIANCE RISKS

AI and Data Governance	
AI Governance Consistency and Integration	Insufficient AI Governance
AI-Drafted Contract Terms Verification	Privileged Access Governance
Data Privacy and Protection Laws	Slow AI Adoption Pace
Controls and Audit	
Compliance Monitoring and Audit Readiness	Internal Control and Oversight
Improper Use of Purchase Cards	Internal Controls, Monitoring, and Audit Readiness
Inadequate Internal Controls	Unauthorized Access
Grant Compliance	
Clawbacks from Non-Compliance	Grant Compliance
Complex Grant Requirements	Non-Reimbursement of Grant Expenditures
FEMA Disaster Recovery Compliance	
Legal, Records and Ethics	
Civil Rights Litigation	Procurement Timeliness vs. Urgent Need
False Arrest	Prohibited Contractor Donations to Campaigns
Fraud, Waste, and Abuse	Public Records and Open Meetings Laws
Improper Asset Disposition	Records Retention
Liability and Compliance	Unauthorized Use of City Seal
Litigation and Claims Risk	Use of Force and Civil Liability
Litigation Hold Execution Gap	Vacant Contract Administrator Roles
Non-compliance with City Charter or City Ordinances	Whistleblower Protections
Procurement and Contracting Compliance	
Adherence to Procurement Laws	Procuring Contracts Under $100K
Procurement and Contracting Compliance	Texas Prompt Payment Act Noncompliance
Regulatory and Policy	
Captioning	Policy Relevance
Changing Regulatory Landscape	Regulatory Compliance Complexity
Labor Law and Employment Compliance	

FINANCIAL RISKS

Cost Inflation and Budget Pressure	
Budget Constraints	Limited Budget Flexibility
Cost Escalation/Cost of Purchases	Overtime Budgeting and Overruns
Cost Overruns	Overtime Costs
Economic Risks	Rising Labor and Benefits Cost
Insurance and Claims Costs	
Financial Accounting Integrity	
ACFR	Litigation Reserve/Budget Adequacy
Error in Cash Handling	Purchase Card Expenditures
Financial Management	Unauthorized Vendor Payments
Grant Management	
Federal Disaster Reimbursement Timing Risk	Grant Funding Uncertainty
Federal Funding Policy Shifts	Oversight of Housing Department Spending and Grants
Financial Oversight for Public Works	Reliance on Grant Funding
Grant Funding Shortfalls	
Procurement Vendor Cost Exposure	
Consolidation of Contracts for Similar Services	Supply Chain Constraints Driven by AI
Reliable Maintenance Contracts	Supply Chain Procurement
Rising fuel, parts and component costs	Technology Spend Fragmentation
Revenue Pressure and Budget Capacity	
Availability of e-materials	Limited Funding
Cable Revenue	Meeting Accreditation
Expense Growth Not Keeping Pace with Revenues	Revenue Projection

Financial Limitations to Workforce Technology
Financial Sustainability/Budget Deficit Risk
Inadequate ability to generate additional revenue
Insufficient Budget Allocation
Lack of reimbursement contracts with insurance providers
Revenue Stream Limitations
Special Revenue Fund Depletion
Structural Budget Imbalance
Underfunding of Critical Infrastructure

HEALTH, SAFETY AND ENVIRONMENT RISKS

Animal Welfare and Zoonotic Risk

Animal Shelter Perception
Public Trust and Confidence
Zoonotic Disease and Animal Control

Public Health and Emergency Readiness

Limited Funding for Public Health Medical Treatment
Major Incident Readiness
Workplace Food and Beverage Access

Workplace Safety, PPE Preparedness

Employee Safety and Operational Continuity
Firefighter Safety Risk and PPE Performance
Safety Requirement Complexity
Security and Safety
Workplace Safety

OPERATIONAL RISKS

Coordination and Communication

Communication and Planning Silos
Cross-departmental Coordination
Interdependency with Partner System
Leadership Coordination
Operational Communication
Siloed Communication
Untimely/Inaccurate Communication

Critical Asset and Infrastructure Lifecycle

Aged Equipment
Aged Fleet
Aged/Inadequate Facilities
Apparatus Age and Condition
Deferred Maintenance
Facilities Management
Infrastructure Resiliency
Not Enough Equipment
TV Station/Plant Modernization
Vehicle Damage

Cyber Resilience and Access Protection

Aging Technology
Cyber Attack
Cybersecurity and System Resilience
Cybersecurity Threats
Lack of Cybersecurity Visibility
Lack of IT security officer
Physical Security for IT Room
Reliance on Technology Vendors
Technical Debt

Lack of Centralized Reporting

Claims Reporting
Grant Monitoring and Reporting
Inventory Reporting
Monitoring IT Access and Permissions

Operational Process

Customer Service
Data-Informed Decision Making
Food Inspection Backlog
Fragmented Risk Management
HR Service Delivery
Inadequate Review of Liquor License Certificates
Lack of Accountability and Ownership
Lack of Coordination/ Collaboration Across City Functions
Lack of Documented Processes
Operational Consistency
Operational Continuity
Operational Inefficiencies due to Lack of Transparency
Permitting Interdependency and Licensing Compliance Deadlines

Procurement Delays

Delayed Invoice Payments
Delayed Procurement
Delays in Payment Processing
Financial Liability from Prolonged Contract Procurement
Inefficient Coordination Related to Procurement
Procurement Prioritization
Slow Approval of Procurements

Staffing Capacity and Service Coverage

Custodian of Records Staffing Limitations
HR Support Challenges
Non-Emergency Call Operations
Planned and Unplanned Event Surge Response
Quality Assurance Deficiencies
Service Level Answer Index
Staffing Constraints
Staffing Shortages
Supervisory Accountability
Understaffed/Under Funded Cybersecurity Program

Recreation, Wellness and After School Programs	Workforce Attraction and Retention
Reduced Budget Allocation for Staffing	
Succession Planning	
Aging Staff in HITS	Workforce Succession Planning
Succession Planning Readiness	
Technology Reliability and Modernization	
Aging and Fragmented Technology Infrastructure	Lack of Housing Software Applications
Capital Improvement Project Delivery Capacity	Lack of System Integration
Climate and Extreme Weather Events	Lacking Pharmacy Inventory System
Court Management System Failure	Language Access and AI Technology Reliability
Cumbersome Management Information System	Manual Entry of Citations
Duplicate Online Payments	Modern Digital Services
Innovation and Modernization Pace	Open Finance Tool
Insufficient Technology	Power and Energy Reliability
Integration of Systems	Technology and Workflow Inefficiencies
Internal and External Technological Application Reliability	Technology and Records Retrieval
IT (General) Risks	Technology equipment shortage
Lack of Automated Processes	Understaffed IT Organizations
Vendor Service Delivery	
Grounds Maintenance	Vendor Services
Vendor and Third Party Compliance	
Workforce Recruitment and Retention	
Attraction and Retention of Mid-Level Employees	Limited Employee Engagement
Collective Bargaining Agreements	Recruitment of Advanced Level Mechanics
Concentrated Institutional Knowledge	Skilled Trades Workforce Shortages
Hiring Constraints and On-Boarding Barriers	Uncompetitive Compensation
IT Recruiting and Retention Challenges	Workforce Attraction and Retention
Job Competition	Workforce Fatigue
Leadership Transition Disruption	
Workforce Training	
Lack of Knowledge	Training and Development
Limited Coaching	

STRATEGIC RISKS

External Disruption and Economic Shifts	
Climate	Industry Consolidation
Geopolitical Risk	Pandemic
Intergovernmental Coordination and Policy Constraints	
County Collaboration Challenges	Misalignment of TIRZ and CoH Priorities
Government Shutdown	Regional Collaboration
Inconsistent Application of Policies	State Constraints on Local Governance
Public Trust, Stakeholder Confidence	
Barriers to Immigrant Community Engagement	Political Manipulation
Community Engagement and Public Trust	Public Awareness of Programs
Marketing	Reputation Risk from a Lack of Transparency
Policy Administration	Reputational Impact of Strategic Failure
Strategic Goal and Priority Alignment	
Identifying Goals and Direction	Misalignment of Citywide Service Delivery Strategy
Identifying KPIs	Strategy Execution Gaps
Inadequate Affordable Housing	

APPENDIX 2: SCORING METHODOLOGY

Each risk was evaluated using three primary dimensions: impact, likelihood, and management preparedness gap. Impact reflects the potential consequence to compliance, financial condition, reputation, and mission or service delivery; likelihood reflects the probability that the risk may occur within the defined planning horizon; and management preparedness gap reflects the extent to which existing controls, policies, processes, and mitigation activities are designed and operating effectively.

The scoring model supports a consistent, risk-based approach by applying common definitions of high, medium, and low ratings across all business areas. Inherent risk is informed by the relationship between impact and likelihood, while residual risk incorporates the management preparedness gap to reflect remaining exposure after considering existing mitigation activities. These criteria help normalize stakeholder input, support comparison across departments and risk categories, and provide a transparent basis for identifying risks that may require additional monitoring, management attention, or consideration during audit planning.

For scoring purposes, qualitative ratings were converted to numeric values to support consistent comparison across departments and risk categories. Impact and likelihood ratings were assigned values of 1 for Low, 2 for Medium, and 3 for High and management preparedness gap ratings were assigned values of 25% for Low, 50% for Medium, and 90% for High.

The Inherent Risk Score represents the level of risk before considering any existing controls or mitigation activities. Inherent risk scores are calculated by multiplying the impact score by the likelihood of occurrence and range from 1 to 9, where higher scores indicate greater exposure.

The Residual Risk Score represents the remaining level of risk after considering the effectiveness of current controls, policies, monitoring activities, and management actions. Residual risk was calculated by multiplying the inherent risk score by the management preparedness gap and range from 0.25 to 8.1. High residual risk represents scores between 5.48 and above, Medium represents scores between 5.48 and 2.87, and Low represents scores below 2.87.

IMPACT

SCORE	COMPLIANCE	FINANCIAL	REPUTATIONAL	MISSION AND SERVICE DELIVERY
High (3)	Material violation of law, ordinance, executive authority, executive order, or administrative policy with significant to systemic implications. Awareness: Public, media, regulators, or external oversight entities.	$15 M or more impact on Operating Cash Flow	Adverse publicity on a regional to national level Severe to substantial damage to reputation Serious or lasting environmental and/or health impact to the community	Significant to widespread disruption of critical or essential services. Prolonged inability to meet statutory, strategic, or public service commitments, with sustained impacts to outcomes, service expectations, and public trust.
Medium (2)	Violation of internal policy and/or department procedures. Awareness: Mayor's Office or City Council	$1 M to less than $15 M impact on Operating Cash Flow	Potential impact to key constituent confidence, brand, and reputation Gets attention of regulators	Measurable disruption to one or more services or programs. Delays, reduced service quality, or localized stakeholder impacts require management attention.
Low (1)	No violation of law, ordinance, executive order, administrative policy, internal policy, or department procedures, or only minor non-adherence to internal guidance or informal practices. Awareness: Limited to department staff, management, or the Department Director level.	Less than $1M impact on Operating Cash Flow	No impact to constituent confidence, brand, or reputation, or limited adverse publicity confined to the local level.	No noticeable impact or only limited, short-term disruption to non-critical services or internal functions. Core mission delivery remains intact, with no effect on outcomes, timelines, or public expectations and minimal stakeholder impact.

LIKELIHOOD OF OCCURRENCE

SCORE	DEFINITION	
High (3)	The future event is highly likely to occur (at least once in a 2-year horizon).	Above 50%
Medium (2)	The chance of the future event is more than unlikely but less than probable (at least once in 3-year horizon).	Between 25% - 50%
Low (1)	The chance of the future event occurring is low (at least once in 10-year horizon).	Less than 25%

MANAGEMENT PREPAREDNESS GAP

SCORE	DEFINITION
High (90%)	Management activities, including controls and policies, are largely absent, ineffective, or not implemented, resulting in an immediate and significant risk exposure.
Medium (50%)	Management activities, including controls and policies, exist but have demonstrated performance issues, resulting in a moderate risk of failure.
Low (25%)	Management activities, including controls and policies, are generally well designed and operating effectively, with minor opportunities to improve

APPENDIX 3: BUSINESS AREA PARTICIPATION

FACILITATED SESSION PARTICIPANTS

Facilitated risk assessment sessions were conducted with key business areas. During these workshops, business area leaders and operational stakeholders reviewed and validated risks identified through the enterprise survey, discussed root causes, mitigation activities, refined risk definitions, and aligned on risk ratings related to impact, likelihood, and management preparedness. These collaborative discussions helped validate enterprise-wide risks affecting service delivery, financial stewardship, compliance, operational resilience, and strategic objectives.

Business areas selected for facilitated group sessions were identified based on the results of the citywide risk identification survey and subsequent risk analysis. Priority was given to departments with complex operations, significant strategic, operational, financial, compliance, or public service responsibilities, and those with risks warranting deeper review and validation.

Facilitated risk assessment sessions were conducted with the following business areas.

- City Controller
- Finance
- Fleet Management Department
- General Services Department
- Housing and Community Development
- Houston Airport System
- Houston Fire Department
- Houston Information Technology Services
- Houston Police Department
- Houston Public Works
- Human Resources
- Legal

SURVEY ONLY PARTICIPANTS

The assessment relied primarily on survey responses submitted through the Citywide risk identification process. These survey results were analyzed and incorporated into the enterprise risk assessment to identify department-specific and cross-cutting risks, enabling representation of these business areas in the City's overall risk profile. The survey-based analysis contributed to the identification of recurring enterprise themes and supported the development of the City's consolidated risk universe and prioritization of enterprise risks.

- Administration & Regulatory Affairs
- City Council
- City Secretary
- Department of Neighborhoods
- Houston Emergency Center
- Houston Health Department
- Houston Parks and Recreation
- Houston Public Library
- Mayor's Office
- Municipal Courts
- Office of Business Opportunity
- Planning and Development

BUSINESS AREAS SOLICITED WITHOUT RESPONSE

Solid Waste Management was solicited but did not provide a response during the assessment period. A detailed business area risk profile was therefore not prepared for Solid Waste Management during this cycle. Related service delivery, operational continuity, workforce, fleet, and financial considerations may be evaluated through future risk assessment and audit planning activities.