Enterprise Risk Assessment and
Fiscal Year 2025 Annual Audit Plan

I.   Enterprise Risk Assessment

The Office of the City Auditor performs enterprise risk assessment (ERA) activities to assess the City's risk exposure and ensure internal audit resources are allocated to audit engagements based on risk. Our professional standards require risk be assessed and the audit plan updated based on risk at least annually.

We assess risk exposure based on the likelihood a risk event would occur, and the impact or significance the risk event would pose for the organization if it did occur. *Inherent risk* describes risk without considering management control activities. *Residual risk* may be lower than inherent risk when management has effective internal controls in place to mitigate inherent risk. Internal auditors are interested in identifying moderate and high inherent risk exposures and determining whether residual risk is at an acceptable level (according to management's risk appetite).

Internal auditors typically track enterprise risk by auditable entity, which is a classification unique to each organization that identifies its key services and operations. The Office of the City Auditor defines the City's auditable entities as the key offices, departments and funds described in the annual budget book. Auditors aggregate risk information by auditable entity over time. Macro risks affecting several or all-auditable entities may result in "citywide" audit engagements.

II.   Approach

In Spring 2024, Internal Audit conducted in-depth enterprise risk assessment discussions with general government management, including charter officers, to identify and assess risks impacting the City. These discussions included focus on the City's strategic goals and objectives, management priorities and initiatives, risks to achieving those objectives and priorities, emerging risks, available resources, and missed opportunities.

In addition to information gathered during performance of audit engagements, some of the sources that help us assess organizational risk include various causes of fraud and investigation matters, staff input, professional and other external resources, emerging risks, and themes of complaints through various intake mechanisms.

Figure 1 defines example risk categories that help facilitate risk conversations with stakeholders.

Figure 1 - Example Risk Categories

Organizational Risk Category	Risk Description
Compliance Risk	Risk of loss due to noncompliance with policies, contracts, agreements, or grants.
Environmental Risk	Risk of loss of life, financial loss, failed services, or missed opportunities due to extreme weather, natural disasters, human-made disasters, loss of biodiversity, etc.
Financial Risk	Risk of loss due to inadequate or ineffective controls around tax, accounting, financial reporting, capital and debt management, investments, and other financial processes.
Fraud, Waste and Abuse Risk	Risk of loss and other consequences due to misappropriation of assets, corruption, or financial statement fraud.
Information Technology Risk	Risk of financial loss and service failure around privacy and confidentiality, security, cybersecurity, cloud computing, mobile device security and IoT, business continuity and disaster recovery, software asset management, user access management, data governance, and remote workplace processes and systems.
Legal and Regulatory Risk	Risk of noncompliance with local, state or federal laws and regulations.
Operational Risk	Risk that City processes and services are not effective or efficient, or not in alignment with City goals and objectives; or human capital is not sufficient to meet operational or business continuity goals.
Public Safety Risk	Risk that communication policies, safety standards, physical security, emergency response training, routine security, and other related process and systems controls are not adequate to sufficiently mitigate safety risk for the public or employees.
Reputation Risk	Risk of decreased quality of services, community engagement, and trust, due to negative word of mouth or other neighbor communications.
Strategic Risk	Risk that the City's strategic priorities are not achieved. *Management goals and objectives should align with the City's strategic priorities.*
Third Party Risk	Risk of financial loss, inability to provide services, data breach, noncompliance with contract terms, or other failure related to third party agreements.

An example of the overall ERA process is depicted in Figure 2.

Figure 2 - Overall Enterprise Risk Assessment Process

For the first time, Internal Audit conducted an Information Technology Risk Assessment of the City. The results of the IT Risk Assessment remain confidential and exempt from pubic record based on *Florida Statute 119.07(2).* Audit engagement(s) were added to the 2024 audit plan and fiscal year 2025 audit plan to address identified risks. The risk assessment was conducted based on the following phased approach:

- IT Risk Assessment Phased Approach
    - Phase I – Identify and understand the enterprise strategy including organization, budget, data flow, risk and controls
    - Phase II – Develop the IT audit universe including processes, organizational structure, policies and procedures, services, infrastructure and applications
    - Phase III – Risk Assess the IT audit universe to include risk scenarios and risk factors. The audit universe comprises thirty three security domains and over 300 applications and peripherals
    - Phase IV – Develop and validate the audit plan based on risk prioritization of processes and applications

Micro Risk Factors

The most significant risks identified included the management of **overall IT risk, cybersecurity risk, and ERP data reliability risk**. IT-related risks were the leading risks communicated by management in our 2024 enterprise risk assessment interviews. Internal Audit completed a phase II cybersecurity audit in 2022.

Staffing and talent management was the next leading concern communicated by management. In 2021, Internal Audit completed a Succession Planning audit to address some of these concerns. All audit issue management action plans have been implemented. Internal Audit monitored the implementation of HR-related action plans from the 2021 Culture Assessment.

Risks related to **procurement** operations and processes were frequently noted by management.

Infrastructure was also high on the list of risks noted.

Other significant risks communicated by management were **regulatory risk** and **budgeting risk**. Changes in the regulatory environment related to utility operations impact budget planning, resources, and operations.

Public safety risk for City workers was communicated as a concern due to recent incidents at the City Hall complex.

Macro Risk Factors

External political, economic and environmental factors, emerging risks, as well as laws and regulations impact our organization's risk exposure. Federal agency partners and professional association research and publications are some of the resources that assist us in identifying key macro risks that may impact the organization. We highlight below a few examples.

The Institute of Internal Auditors (IIA)
In the IIA's Risk in Focus 2023 report, the following areas are noted as five top organizational risks for 2024: **Cybersecurity**; **Human Capital; Regulatory Change;** Market Changes; **Business Continuity.**
https://www.theiia.org/en/content/communications/press-releases/2023/september/internal-audit-foundation-releases-first-of-its-kind-global-risk-in-focus-reports/

Figure 3 – Institute of Internal Auditors Top Risks to Organizations in 2024 and 2027

Current risk levels vs. future risk levels – North America

Future risk

- Cybersecurity and human capital dominated the risk landscape for North America for 2024.
- In the next 3 years, digital disruption and climate change are the risks expected to increase the most.

What are the top 5 risks your organization currently faces?

Risk	%
Cybersecurity	85%
Human capital	65%
Regulatory change	43%
Market changes	41%
Business continuity	36%
Digital disruption	36%
Supply chain and outsourcing	36%
Geopolitical uncertainty	28%
Financial liquidity	28%
Communications/reputation	21%
Organizational culture	21%
Health and safety	17%
Governance/corporate reporting	16%
Climate change	12%
Fraud	9%
Mergers and acquisitions	8%

What are the top 5 risks your organization will face 3 years from now?

Risk	%
Cybersecurity	73%
Human capital	51%
Regulatory change	50%
Market changes	38%
Business continuity	25%
Digital disruption	56%
Supply chain and outsourcing	31%
Geopolitical uncertainty	30%
Financial liquidity	20%
Communications/reputation	13%
Organizational culture	21%
Health and safety	12%
Governance/corporate reporting	18%
Climate change	30%
Fraud	10%
Mergers and acquisitions	12%

Source: https://www.theiia.org/en/content/communications/press-releases/2023/september/internal-audit-foundation-releases-first-of-its-kind-global-risk-in-focus-reports/
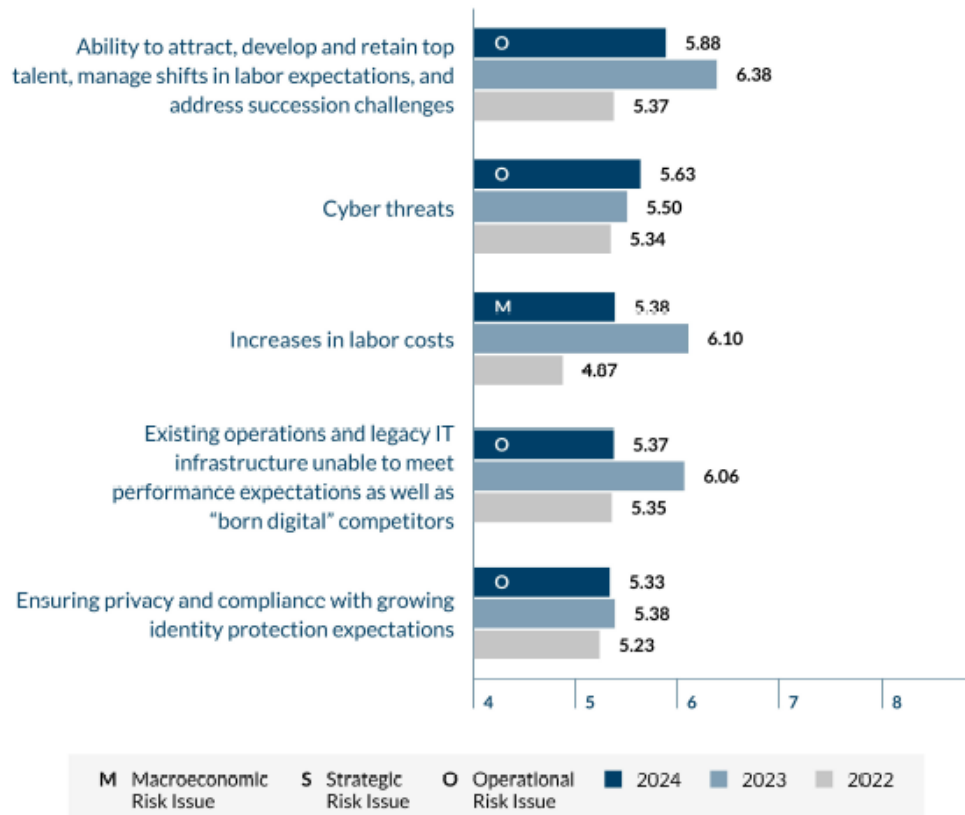
Protiviti

Protiviti, in conjunction with NC State University, released "Executive Perspectives on Top Risks" for 2024 and 2034 based on survey responses from board members and executives worldwide. The top five 2024 risks identified include: **Talent management** (attracting, recruiting, and retaining skilled workers); **Cybersecurity** threats; **Increasing Labor costs**; **Legacy IT** (addressing aging IT infrastructures); **Privacy and Compliance for Identity Protection**. See Figure 4.
Source: https://www.protiviti.com/us-en/survey/top-risks-government-services-2024

Figure 4 – Protiviti Top Risks in Government 2024

Government — 2024

Source: https://www.protiviti.com/us-en/survey/top-risks-government-services-2024

LexisNexis

LexisNexis released 2024 Top Threats in the Public Sector related to cybersecurity to alert governments of cybersecurity and fraud threats. Top 2024 risks include: Fraud-as-a-Service (hired criminals committing fraud; Account Takeover by Synthetic Identities; Artificially Intelligence Fraud; **Serious Cyber threats**; Windows Ransomware.

Source: https://risk.lexisnexis.com/insights-resources/infographic/2024-top-fraud-trends-and-threats-in-the-public-sector

III.   Comprehensive Plan, Strategic Goals, and Management Requests

During planning for every internal audit engagement, the auditor includes an assessment of risk for the process(es) in scope, including alignment with regulations, strategic goals, and policy as applicable.

City leadership and management may request specific audits or advisory services at any time. The City Auditor will work such requests into the audit plan upon approval of the Audit Committee and City Commission, and they will be prioritized with existing engagements on the audit plan.

IV.   Annual Audit Plan

The Annual Audit Plan detailing the engagements planned for review during fiscal year 2025 is depicted in Figure 5.

Enterprise Risk Assessment and
Fiscal Year 2025 Annual Audit Plan

Figure 5 – FY 2024-2025 Annual Audit Plan

Auditable Entity	Proposed Audit Engagement Name	Audit Service Type	Proposed Audit Objective	Estimated Internal Audit Budget
Citywide - General Government	Asset Management Processes	Audit	Assess processes and controls around City assets to ensure they are properly tracked, managed, and accounted for.	500
City Manager	Capital Impovement Planning	Audit	Review plans to ensure resources are adequately allocated to improve infrastructure at greatest risk to impact neighbor and community builder health and safety and to ensure reliable delivery of services over time.	800
Financial Services	Procurement Audit	Audit	Determine whether processes and procedures around the procurement process are efficient, effective, and in compliance with bidding requirements and other applicable guidelines.	600
Human Resources	HR Recruiting and Hiring Processes	Audit	Assess the design and operating effectiveness of the processes and controls related to recruiting and hiring talent.	500
Wild Spaces Public Places	WSPP Project and Fiscal Management	Audit	Review the policies, procedures, and internal controls around Wild Spaces Public Places project and fiscal management processes.	400
Parks, Recreation, and Cultural Affairs	PRCA Billing and Collections (carryover from 2024)	Audit	Evaluate PRCA internal controls for billing and collections processes and merchant account handling.	125
City Manager	ARPA Phase II Reporting Compliance Audit	Audit	Assess effectiveness of ARPA grant program reporting internal controls and use of funds.	300
Financial Services, HR, Technology	Workday Privileged Access (carryover from 2024)	IT Audit	Review whether user access permissions are requested by user management, approved by information owners, implemented by designated access control specialists, and are the minimum permissions needed by the users to do their jobs.	125
Financial Services	PCI Process Audit	IT Audit	Review processes and controls around the governance, effectiveness, and efficiency of PCI DSS security requirements across General Government, including the management of services that are delivered by external providers.	400
Confidential	Data Management	IT Audit	Assess compliance with applicable cybersecurity laws, regulations, and security requirements relating to the creation, viewing, modification, transmission, dissemination, storage, and/or destruction of information.	500
Housing	SHIP and Local Housing Assistance Plan Audit	Audit	Audit use of SHIP funds and adequacy of Local Housing Assistance Plan intended to produce and preserve affordable homeownership and multifamily housing.	200
Ongoing Audit Activities	N/A	Ongoing Audit Services	Audit issue follow-up, enterprise and IT risk assessments, special requests, periodic monitoring, investigations, quality assurance, and Audit Committee activities. Risk additions to the audit plan through out the year.	1958

Total Audit Plan Budgeted Hours: **6,408**

AVAILABLE TEAM HOURS PER 12 MONTH PERIOD	
Non-Admin Budget	**Hours**
City Auditor (1)	1,080
Assistant City Auditor (1)	1,080
Audit Manager (2)	2,808
Internal Auditor (1)	1,440
2024-2025 Internal Audit Team Total Available Hours (12 month period):	**6,408**

Thank You from the Internal Audit Team!

Our Internal Audit Team

     Stephen Mhere, CIA, CISA, MBA, MS, City Auditor

     Brecka Anderson, CIA, CFE, CGAP, Assistant City Auditor

     Diana Ferguson-Satterthwaite, FCCA, CIA, CFE, Audit Manager

     Lisa, Siedzik, CISA, IT Audit Manager

     Peter DeMaris, Internal Auditor and Lead Auditor for this Engagement

     Meayki Batie, Audit Coordinator