



# Proposal for Independent IT Audit Services ITN No. 2024-05

City of Doral

April 10, 2024

Reema Parappilly, CISA | Partner, IT Advisory Services  
Weaver and Tidwell, L.L.P.  
832.320.3254 | reema.p@weaver.com





# CONTENTS

**Letter of Transmittal..... 1**

**Qualification Statement..... 2**

**Approach and Methodology ..... 12**

## Letter of Transmittal

April 10, 2024

City of Doral

RE: Proposal for Independent IT Audit Services – ITN No. 2024-05

On behalf of Weaver and Tidwell, L.L.P. (Weaver), I am pleased to submit our Proposal for Independent IT Audit Services – ITN No. 2024-05. We appreciate the opportunity to earn your business and your trust.

**Weaver has provided assurance and advisory services to government entities for nearly 75 years. With 21 offices from coast to coast and nearly 1,700 professionals, we're committed to helping clients like the City of Doral reach their IT security goals.**

**At Weaver, there are no “one-size-fits-all” solutions. We combine leading technical knowledge with specific industry experience to provide highly customized services tailored to each client's needs.**

### Industries

- ▶ Government
- ▶ Not-for-profit
- ▶ Higher Education
- ▶ Real Estate
- ▶ Construction
- ▶ Hospitality & Entertainment
- ▶ Health Care
- ▶ Professional Services
- ▶ Private Equity
- ▶ Insurance
- ▶ Technology
- ▶ Blockchain & Digital Assets
- ▶ Alternative Investments
- ▶ Financial Services
- ▶ Banking
- ▶ Manufacturing
- ▶ Distribution & Logistics
- ▶ Oil & Gas
- ▶ Energy Transition & Renewables

### Services

- Advisory Services**
  - ▶ Risk Advisory Services
  - ▶ IT Advisory Services
  - ▶ Digital Transformation & Automation
  - ▶ Government Consulting Services
  - ▶ Asset Management Consulting
  - ▶ Accounting Advisory Services
  - ▶ Transaction Advisory Services
  - ▶ Valuation Services
  - ▶ Forensic & Litigation Services
  - ▶ Family Office Services
- Assurance Services**
  - ▶ Audit, Review & Compilation
  - ▶ Agreed-Upon Procedures
  - ▶ Employee Benefit Plan Audit
  - ▶ SOC Reporting
  - ▶ Attestation Services
  - ▶ IFRS Assessment & Conversion
- Tax Services**
  - ▶ Federal Tax
  - ▶ State & Local Tax
  - ▶ International Tax
  - ▶ Personal Client Services



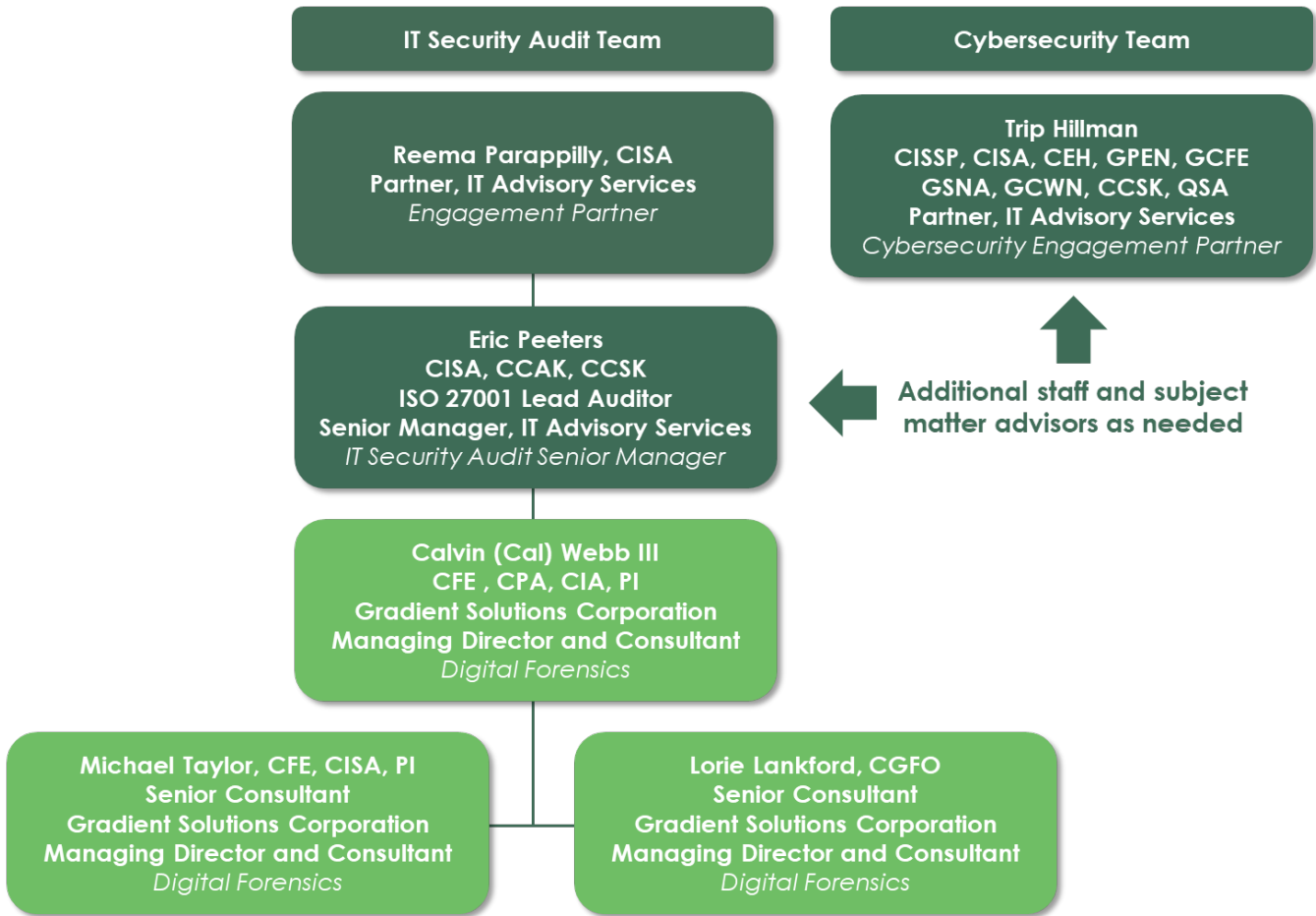
We appreciate the opportunity to earn your business and your trust. If you have any questions about our proposal, please feel free to contact me directly.

Sincerely,

Reema Parappilly, CISA | Partner, IT Advisory Services  
Weaver and Tidwell, L.L.P. | 4400 Post Oak Parkway, Suite 1100 | Houston, TX 77027  
832.320.3254 | reema.p@weaver.com

# Qualification Statement

a. Organizational Chart: The organizational structure of relevant teams and personnel is provided below. Those listed have been selected for their deep knowledge and wide-ranging experience in the focus areas prioritized by the City. Their experience is detailed in **c. Project Team’s Experience** section below.





b. Proposer's Experience: Provide a listing of projects within the last 5 years where the Proposing entity has provided services similar to those described herein. The determination of similarity shall be solely at the City's discretion.

Please refer to the references provided in **Attachment A**. Out of respect for the privacy of our clients, we defer the provision of additional details regarding client projects until the next phase of the selection process. At that stage we will facilitate contact with additional clients.

c. Project Team's Experience:



**Reema Parappilly, CISA, CDPSE | Partner, IT Advisory Services**

Reema has more than 18 years of experience providing IT advisory services. Her focus includes IT internal audits, external audit support, continuous controls monitoring and Sarbanes-Oxley Compliance. She has experience performing IT risk assessments and executing IT internal audit plans, including strategic electronic asset management, database administration (Oracle, SQL Server, MySQL), data loss prevention, remote technology (post-COVID assessment) and system implementations. She also leads compliance engagements, including annual documentation of controls design and testing. Her focus is always on helping clients balance compliance with organizational resource restrictions and to enable process owners to improve decisions regarding internal controls.



**Representative Client Experience**

- City of Houston
- City of Bryan / Bryan Texas Utilities
- City of Corpus Christi
- Calif. State Teachers' Retirement System
- Employees Retirement System of Texas
- Texas Lottery Commission
- Texas Department of Insurance
- Houston ISD
- Montgomery ISD
- Austin Community College District
- Alamo Colleges District
- College of the Mainland
- Lee College
- IBM Cloud
- Callon Petroleum Company
- TEAM, Inc.

**Professional Involvement, Additional Certifications and Education**

- Member, ISACA, IIA, Insurance Accounting and Systems Association (IASA), Cloud Security Alliance (CSA) and AFCOM International
- CISA and Certified Data Privacy Solutions Engineer (CDPSE)
- Master of Science, Information Systems Technology, and Bachelor of Business Administration, Finance and Information Systems, George Washington University

**Representative Presentations and Publications**

- "Diversity in Security" Luncheon Speaker, Cloud Security Alliance's 2022 Annual SECTember Conference
- "Don't Have Your Head in the Clouds on Cloud," Association of Public Pension Fund Auditors (APPFA) Fall Conference
- "Application Implementations: How IA Can Save the Day," Texas State Auditor's Office
- "Cyber Attacks: How Prepared Are You?" TXCPA School District Conference
- "How to Reduce Terminated User Exceptions in Your Next Audit," Weaver Blog



**Eric Peeters, CISA, CCAK, CCSK, ISO 27001 Lead Auditor | Senior Manager  
IT Advisory Services**



Eric has over 15 years of experience in IT advisory and operations experience with significant knowledge of cloud services providers and users. He often works in complex, highly technical environments and consults with local and state government entities, global cloud providers, Fortune 100 companies, private equity groups and start-ups.

Eric's experience linking technology environments to governance and compliance requirements enables him to advise clients on attaining and maintaining certifications and attestations over Payment Card Industry Data Security Standards (PCI DSS), Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR), ISO 27001 and 27018, National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), and System and Organization Controls (SOC). He has also performed multiple internal audit and consulting engagements, managing acquisition or implementation of Enterprise Resource Planning (ERP) and large public administration software.

**Representative Client Experience**

- City of Dallas
- Texas Department of Motor Vehicles
- California State Teachers' Retirement System (CalSTRS)
- IBM & SoftLayer
- Pavaso
- VALID Systems
- Audax Private Equity
- Range Resources Corporation
- First Command Financial Services

**Professional Involvement, Additional Certifications and Education**

- Member, CSA, IIA and ISACA
- Certified ISO/IEC 27001 Lead Auditor
- CISA, CCAK, and CCSK
- Bachelor of Business Administration, Business Information Systems, and Bachelor of Business Administration, Accounting, Texas Christian University

**Representative Presentations and Publications**

- "Don't Have Your Head in the Clouds on Cloud," Association of Public Pension Fund Auditors (APPFA) Fall Conference
- "What AI Won't Tell You About Implementing AI," ISACA North Texas
- Weaver Foundational Fridays – A Virtual Cybersecurity CPE Series
  - "How Do You Secure What Exists for Two Minutes? The New Cybersecurity Basics in the Cloud!"
  - "From Chaos to Control, Unraveling the Art of Incident Control"



**Trip Hillman, CISSP, CISA, CEH, GPEN, GCFE, GSNA, GCWN, CCSK, QSA | Partner, IT Advisory Services**

Trip has more than 12 years of hands-on experience evaluating IT security. He performs IT vulnerability assessments, IT audits and penetration tests, and has performed and led over 200 audits across hundreds of unique IT environments. He is often engaged to help organizations evaluate their overall security posture and develop prioritized, balanced roadmaps for increasing security maturity.



Trip remains at the forefront of best practices, regulatory requirements and leading frameworks (including COBIT, NIST-CSF, CIS CSC and ISO 27001).

Trip teaches security auditing classes across the nation for the SANS Institute, the leading research and education organization for security professionals.



**Representative Client Experience**

- City of Dallas
- University of Texas System
- University of Texas Arlington
- Austin Community College District
- College of the Mainland
- Blinn College
- Austin Water
- **\*\*Confidential\*\*** Regional Water District
- Calif. State Teachers' Retirement System
- Texas General Land Office
- Employees Retirement System of Texas
- Cancer Prevention and Research Institute of Texas
- North Texas Tollway Authority
- Dallas ISD
- Fort Worth ISD
- IBM Cloud

**Professional Involvement, Additional Certifications and Education**

- Member, International Information Systems Security Certification Consortium (ISC2), ISACA, Institute of Internal Auditors (IIA) and Cloud Security Alliance (CSA)
- Instructor, SANS Institute
- Bachelor of Business Administration, Management Information Systems, Baylor University



## Digital Forensics Team: Gradient Solutions Corporation



### **Calvin (Cal) Webb III, CFE, CPA, CIA, PI | Managing Director and Consultant**

Cal is a capable leader with a broad business background of 18+ years in numerous sectors covering executive leadership as a Chief Financial Officer, an audit background, and significant business consulting experience specifically with Gradient Solutions Corporation. Cal enjoys building and maintaining relationships with co-workers, stakeholders, and clients to help meet and solve difficult business problems in the most effective and efficient means possible. During his time at Gradient, Cal has been an active speaker at professional organizations and industry trade groups including the Government Finance Officers Association of Texas, the Texas Municipal League, the Association of Local Government Auditors, the Association of Government Accountants, the Association of County Auditors, and several other organizations.



Besides Gradient, Cal has worked with Deloitte in external audit and Viziv Technologies LLC as the CFO. During Cal's tenure as the CFO of Viziv Technologies, LLC, he oversaw three external audits from a top-10 firm, quarterly 409A valuations from a top-10 firm, a complex international tax structure (multiple countries, 20+ entities, complex 1065), international compliance processes including KYC and FCPA requirements, accounting, treasury, human resources, tax, procurement, and finance.

With Gradient, Cal has performed multiple consulting projects and internal audits covering a wide range of operations for cities, including a municipal court, utility operations, performing arts center, golf course, airport, recreation venue and convention center. He has experience in consulting relating to grant funds originating from all types of federal and state grantors with requirements from 2 CFR 200 and related Texas requirements. His clients have included the North Central Texas Council of Governments (NCTCOG), Dallas County, City of Irving, City of Arlington, City of Frisco, City of Mesquite, City of Richardson, City of Southlake, City of Round Rock, and many others.

### **Professional Involvement, Education and Certifications**

- CPA, CIA and CFE
- Licensed private investigator (PI — TX/94773802).
- Certified Desktop Specialist, Tableau Software
- Master of Accountancy and Bachelor of Business Administration, Accounting, Baylor University



**Michael Taylor, CFE, CISA, PI | Senior Consultant, Gradient Solutions**

Michael is a Senior Consultant for Gradient Solutions Corporation specializing in data analysis, third-party risk, and IT governance and security. His more than 18 years of experience leading effective teams in both the public and private sectors provide a deep insight into group dynamics, human behavior, and organizational oversight. During his tenure with Gradient, Michael has been an active speaker on information controls and security as well as the use of data in reducing risk and improving oversight. He regularly participates in internal control reviews, data analysis engagements, digital evidence analysis, and third-party risk assessments. His clients have included City of Fort Worth, the North Central Texas Council of Governments, City of Frisco, City of Richardson, City of Southlake, several large non-profits, and others.



Prior to joining Gradient, Michael spent six years in leadership with a small technology start-up in North Texas, Viziv Technologies. First as Chief Administration Officer and then as Executive Vice President for Support Operations, Michael oversaw the company's security, communications, information systems, government affairs, facilities infrastructure, and administrative functions. His private sector experience was preceded by nine years as a congressional staffer in the United State House of Representatives. Active roles in policy research, legislative negotiation, public hearings, community engagement, and office management ran parallel with his responsibilities in information systems management for the Sixth Congressional District's Washington, D.C., office and three district offices.

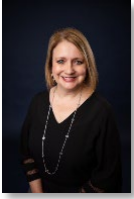
Michael's diverse professional experience has led to a firm understanding that outcomes improve when solutions are collaborative, risk-informed, and driven by real data. This is the essence of Gradient Solutions.

**Professional Involvement, Education and Certifications**

- Certified Fraud Examiner (CFE)
- Certified Information Systems Auditor (CISA)
- Licensed Private Investigator (TX/0093095)
- Bachelor of Science, Agribusiness, Texas A&M University

**Representative Presentations**

- "Your Role as a Fiduciary and Risk Assessor," New and Emerging Finance Directors Training (NCTCOG), September 2021
- "Data Analytics," New and Emerging Finance Directors Training (NCTCOG), September 2021
- "Fraud and Internal Control," Municipal Finance for Non-Finance Directors (NCTCOG), April 2022



**Lorie Lankford, CGFO | Senior Consultant, Gradient Solutions**

Lorie is a Senior Consultant for Gradient Solutions Corporation specializing in local government finance, internal controls, and reporting. She has more than 25 years of experience in the field. Lorie started her career with the City of Georgetown, TX where she worked for 14 years. While there she progressed from Staff Accountant to Controller. She managed the city's accounts payable, payroll, budget and financial reporting functions. Lorie then spent 8 years as the Deputy Chief Financial Officer for the City of Round Rock, TX. She managed the same accounting functions, as well as, utility billing department, economic development incentive agreement compliance, sales tax rebate monitoring, and ERP implementation. Between her tenure at Round Rock and joining Gradient, Lorie has been sharing her breadth and depth of knowledge with various local government finance departments as a consultant focused on special projects, mentoring, and operational improvements.

Lorie served on the board for Government Finance Officers of Texas for 3 years as Central Texas Representative for the organization. She also served as the chair of the Certified Government Finance Officers (CGFO) committee for several years. The CGFO program is an educational program designed to verify knowledge in various areas of government finance. Lorie had an active role in reviewing, updating, and automating the CGFO exam.

At Gradient, Lorie has started providing valued executive-level advisement to clients in their financial operations and is beginning to participate in internal audit related projects. Lorie is excited to begin expanding her focus in the world of forensics and plans to pursue certification beginning sometime in the Summer of 2024.

**Professional Involvement, Education and Certifications**

- Certified Government Finance Officer
- Bachelor of Business Administration in Accounting, Texas State University
- Graduate of ICMA High Performance Leadership Academy

## Certifications and Industry Involvement

This engagement will be staffed leveraging our highly experienced, full-time professionals that stay at the forefront of the industry through ongoing certifications. Some of the many certifications held by our team includes:

- ▶ Certificate of Cloud Security Knowledge (CCSK)
- ▶ Certification in Risk Management Assurance (CRMA)
- ▶ Certified Cloud Security Professional (CCSP)
- ▶ Certified Data Privacy Solutions Engineer (CDPSE)
- ▶ Certified Ethical Hacker (CEH)
- ▶ Certified Fraud Examiner (CFE)
- ▶ Certified Government Auditing Professional (CGAP)
- ▶ Certified HITRUST CSF Practitioner (CCSFP)
- ▶ Certified in Risk and Information Systems Control (CRISC)
- ▶ Certified Information Systems Auditor (CISA)
- ▶ Certified Information Systems Manager (CISM)
- ▶ Certified Information Systems Security Professional (CISSP)
- ▶ Certified Internal Auditors (CIA)
- ▶ Certified ISO 27001 Lead Auditor
- ▶ Certified Public Accountant (CPA)
- ▶ Chartered Global Management Accountant (CGMA)
- ▶ Cybersecurity Maturity Model Certification Registered Practitioner (CMMC RP)
- ▶ GIAC Certified Windows Security Administrator (GCWN)
- ▶ GIAC Forensic Examiner (GCFE)
- ▶ GIAC Penetration Tester (GPEN)
- ▶ GIAC Systems and Network Auditor (GSNA)
- ▶ Payment Card Industry Professional (PCIP)
- ▶ PCI Qualified Security Assessor (QSA)
- ▶ AICPA Advanced SOC for Service Organizations Certificate



Our professionals also stay abreast of best practices, industry trends and compliance issues through active participation in numerous professional and industry associations.

- ▶ Member, Information Systems Audit and Control Association (**ISACA**), Board Member (North Texas Chapter), Past President (North Texas Chapter) and Vice President – Education (North Texas Chapter)
- ▶ Member, International Information Systems Security Certification Consortium (**ISC2**)
- ▶ Executive Committee Member, American Institute of Certified Public Accountants (**AICPA**) Information Management and Technology Assurance (**IMTA**)
- ▶ Chair, Cybersecurity Task Force, IMTA Executive Committee
- ▶ Member, Cloud Security Alliance (**CSA**), Trusted Cloud Consultant (**TCC**), Certified STAR Auditor, Working Group Team Leader - Cloud Controls Matrix (**CCM**) mapping to National Institute of Standards and Technology (**NIST**) Cybersecurity Framework (**CSF**)
- ▶ SOC Task Force, AICPA Information Technology Executive Committee (**ITEC**)
- ▶ AICPA SOC for Service Organization School Graduate and Presenter at AICPA's National SOC School
- ▶ Member, International Association of Privacy Professionals (**IAPP**)
- ▶ Member, Federal Bureau of Investigation (**FBI**) InfraGard Chapter
- ▶ Member, Michigan Council of Women in Technology Foundation
- ▶ Member, **Tech Titans** and Tri-Chair, Cybersecurity Forum of Tech Titans

## Approach and Methodology

---

a. Technical Approach: An outline of the vendor's technical approach to conducting the IT security audit, including the methodologies, tools, and techniques they will employ.

Your Weaver team is keenly aware of the complexities and nuances involved in managing government IT investments. As the foundation of our procedures, we evaluate design and controls in the context of how you operate and consider the structure, systems, third parties and tools available.

From seasoned partners to the newest associates, all Weaver professionals understand that our commitment to quality requires thoughtful planning, consistent follow-through and attention to detail. We start by ensuring that staff have the knowledge and experience required to carry out their responsibilities. Recognizing that supervisors and other reviewers can complement that knowledge, our policies and procedures also provide for consultation with Quality Risk Management on significant matters and multiple layers of technical review.

To meet, and more importantly demonstrate, that commitment to quality, we perform our engagements according to a well-defined structure:



### Phase 1: Planning

First, we perform planning procedures to ensure we develop the appropriate scope and objectives that align with the City's focus areas and risks and ensure that appropriate criteria are developed. Based on the nature and duration of the engagement, we will establish a detailed project plan with the engagement assumptions. The plan will include responsibilities, milestones, and deadlines applicable both to the Weaver team as well as the City to ensure that information flows timely in both directions and that each team understands the other's needs and capabilities in order to meet the City's overall objectives and execute according to the agreed upon timeline.

We'll also determine the frequency of status meetings. We typically hold either weekly or bi-weekly status meetings based on the nature and duration of the project. The status meetings include the status of evidence requests, testing, preliminary issues and any significant items for discussion based on our procedures.

## Key Planning Objectives

In order to maximize efficiency during fieldwork, avoid unnecessary work and reduce the risks of delays in execution, we will work collaboratively with City staff during our planning phase to ensure that all questions related to the purpose, stakeholders, and data relevant to our procedures are identified before fieldwork.

Key tasks performed at this stage will include:

- ▶ Ensuring alignment on goals of the internal audit - with the core understanding that this initiative comes in response to recent concerns of the City that folders designated as private and restricted were improperly accessible due to permission inheritance issues, and that all City employees are in-scope for the audit.
- ▶ Identifying relevant City IT Security Policies and Procedures governing access to folders and systems in scope, and identify personnel responsible for the operational implementation and enforcement of the identified policies, procedures, and/or standards.
- ▶ Identify personnel and/or vendors with the necessary system privileges to grant us access to the data required to perform the in-scope activities.
- ▶ Reviewing prior audits over file structure or information security performed at the City since 2018, and discuss with relevant personnel whether and how findings from the audits were remediated.
- ▶ Discussing with relevant City personnel any potential focus areas of folders, teams, or personnel based on prior instances of inappropriate access to files and data, results of efforts to identify the root cause of inappropriate access, and subsequent measures implemented to reduce the risks of re-occurrence; and
- ▶ Discussing with relevant City personnel state and local regulations or mandates impacting the handling of data and the sharing and distribution of our findings and recommendations.

Based on the outcomes of the above activities, we will finalize scope and objectives of the internal audit and design relevant and appropriate procedures to be executed during the Fieldwork phase.

### Phase 2: Fieldwork

#### Review of IT Security Policies and Procedures

Our experience tells us government entities do not consistently document controls, though the control activities are being executed. Adequately describing who performs a control activity

and how frequently is a starting point, but well-documented controls also include the following elements to assist the function in understanding the purpose of the internal control:

- ▶ The specific attributes contemplated during the execution of a control or process
- ▶ Assessment of the accuracy and completeness of the underlying reports or data
- ▶ The types or nature of errors that the control is designed to prevent or detect
- ▶ Testing of the accuracy and completeness of system-generated data and reports

Where controls don't exist but practices appear to be in place for folder and data access management, we will test the processes that implement the practices with the same rigor and the same approach we would for fully documented controls.

Our review of the City's existing IT Security Policies and Procedures will involve a three-step approach:

### Step 1

- ▶ As it relates to user administration, we will assess the breadth and coverage of policies and procedures against relevant categories of the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF). NIST recently released version 2.0 of the CSF, which includes a new function around the governance of IT security practices, making the framework well-suited to assess the operational practices in place at the City to protect information, and also the governance and oversight activities over the practices. Our reliance on NIST CSF provides a well-established, recognized baseline to ensure your policies, procedures, and processes comprehensively address the risks your controls are mitigating against.
- ▶ The new CSF 2.0 includes a dedicated Governance function, with categories and subcategories dedicated to assessing risks to information, assigning roles and responsibilities over security practices, managing vendors, and enforcing, and monitoring policies and procedures.
- ▶ We will work with City personnel during the Planning phase of the engagement to define the relevant categories and subcategories and ensure that we assess the City at a level that is appropriate for the City's needs, risk appetite, and capabilities.

### Step 2

- ▶ We will review the policies, procedures, and controls of the City against the Identify, Protect, Detect and Respond functions of the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) to ensure that the key elements of operational security are translated into planned practices at the City. The purpose of the review will be to determine whether the City's operational security plans encompass the practices and activities that are called for by the CSF. Our procedures



will ensure that we look beyond the implementation of operational measures to how these measures are managed, updated, and tracked for effectiveness.

- ▶ Where a gap exists, we will discuss with City personnel to understand the rationale for the gap, and whether other procedures are in place to either close or mitigate the gap.

### Step 3

- ▶ We will perform audit procedures to confirm that the IT Security policies, procedures, and/or controls previously identified are in place. To gain efficiencies and time, we will perform audit procedures only where our planning activities have informed us that processes are in place and audit evidence is available. For policies, procedures, and/or controls not supported by processes, we will reach the appropriate conclusions and include them in our report together with recommendations for remediation.

Specifically for folder permissions, we will examine all permissions set on such folders since 2018 and perform fieldwork from two different aspects:

- What *could* go wrong?
- What *did* go wrong?

For the “What *could* go wrong?” perspective, we’ll consider the following:

- 1. Scope Definition:** Determine the scope of the analysis, including the folders, systems, and users to be included, and encompass folders across different platforms and locations as required.
- 2. Access Controls Assessment:** Evaluate access controls to folders, including user permissions, group memberships and role-based access. This includes ensuring that access rights are assigned based both on authoritative documents when they exist, and on the principle of least privilege to minimize the risk of unauthorized access.
- 3. Data Classification Review:** Optionally, we may analyze the classification of data within folders to ensure sensitive information is appropriately identified and protected. This includes verifying that classification labels are applied consistently and in accordance with organizational policies.
- 4. Security Measures Examination:** Assess security measures implemented to protect folders from unauthorized access, data breaches and malware. This may include encryption, antivirus software, intrusion detection systems and logging mechanisms.
- 5. Audit Trail Analysis:** Review audit trails or logs to track access to folders and monitor changes made to files or permissions. This includes looking for any suspicious activities or policy violations that may indicate security incidents.

We also recognize that administrative access grants access implicitly to folders and data and

will consider how administrative access is managed and who has had the privileged access for the audit period.

For the “What *did* go wrong?” perspective we will:

- ▶ Analyze creation dates for all such folders within the file share
- ▶ Document all instances when permissions were changed or occasions when security-related actions were logged since 2018
- ▶ Review access logs for folders by users who were not the designated mayor, council member, or staff
- ▶ If possible, identify whether documents or data accessed by unauthorized internal or external users were copied, moved, uploaded, or downloaded

We will prepare a detailed timeline of all instances of access, including the specified user, from January 1, 2018, through the present date, including the first and last recorded accesses, and further addressing the following:

- ▶ Specify when folders were created and what permissions were initially granted
- ▶ Identify all instances where changes were made in permissions for each folder within the file share, including identification of which changes in permissions were made
- ▶ Indicate all instances where elected officials or their staff accessed folders belonging to other council members
- ▶ Identify any instances of access by external (unauthorized) users

### Digital Forensics

Weaver will plan to execute the IT security audit; if necessary and based on the finalized objectives, we need to utilize additional digital forensic support, we may seek support from Gradient Solutions Group (Gradient) or a permitted private investigator entity of Florida to perform work that would require such a designation. The Weaver team leverages the professionals from Gradient who have specific experience in recovering digital evidence, including data that someone attempted to delete.



### Gradient Solutions Corporation: Our Digital Forensics Partner

Gradient Solutions is a customer-centered firm driven to protect its clients through risk-focused consulting. Since its founding in 2003, it has specialized in helping public sector, higher education, and not-for-profit entities reduce risk and improve oversight. Gradient understands the unique set of challenges inherent in these environments and offers solutions specific to its clients' needs. Their specialties include risk management, data analytics, information technology, internal audit and compliance, investigations, and training. It seeks to be a trusted resource, operating behind the scenes to help its clients identify the best solutions for their organization.



Gradient has a long history of supporting internal audit and compliance professionals in helping manage risk and improve organizations. Its business consultants have more than 50 years of experience and have served in roles such as audit partner, Municipal Finance Director, CFO and Executive VP. Their team brings knowledge from decades of local government experience to help organizations assess and improve governance, processes and internal controls. They have also worked with numerous organizations to perform risk assessments, train on business and fraud risk, and assist in implementation of risk management strategies. Gradient is licensed as a Private Investigation Company under the Texas Private Security Statutes and Rules Sec. 1702.104. Gradient's license number is A14770801. (Gradient is not a public accounting firm.)

From initial acquisition of evidence to evidence-handling protocols to evidence processing, examination and reporting, the digital forensics team will work with the City and its counsel on some of the City's most sensitive issues. The digital forensic technology utilized can provide the kind of context and perspective to any investigation that traditional paper records alone cannot always fulfill.

### **Forensic Imaging**

The forensics team includes professionals with specific experience in gathering and analyzing digital evidence, including data that someone attempted to delete. While we do not anticipate performing analysis over cell phones, tablets, social media or personal cloud storage accounts, the team has experience imaging various forms of digital data to be analyzed and maintained as evidence, including:

- ▶ Laptop and desktop computer hard drives
- ▶ Data (including email) housed on servers or in the cloud
- ▶ Tablets
- ▶ Cell phones and text messaging data
- ▶ Thumb drives or flash drives

We work with our clients and their counsel on some of their most sensitive issues throughout the forensic imaging process:

- ▶ Initial acquisition of the evidence (typically onsite)
- ▶ Evidence-handling protocols (chain of custody)
- ▶ Evidence imaging, processing and examination

---

The digital forensic technology can provide context and perspective to any investigation that traditional paper records alone can't always fulfill.

---

### Phase 3: Reporting

Focusing on the key technology risks that impact you, we leverage industry guidance to develop our conclusions and recommendations. We will document findings, observations, and recommendations in the audit report. This will provide clear and actionable recommendations to address any identified deficiencies or areas for improvement. Our assessment considers the current state of technology, with a focus on assisting you in validating the existence of or need for the following components of a mature IT control:

- ▶ A robust and secure IT infrastructure
- ▶ Appropriately defined and verified controls
- ▶ Processes and policies that implement the controls
- ▶ Complete documentation that demonstrates control implementation
- ▶ Employees who understand and follow the processes

We'll formally discuss our results with the relevant stakeholders at an end-of-fieldwork meeting, and also during an exit meeting. Our team is experienced with tailoring reports to the intended audience, ranging from a granular, step-by-step document for operational staff to allow them to identify the specific issues we report on, to high-level, risk-focused reports for City leadership.

We'll provide the City a report that includes management's action plans and a planned implementation date, which will be incorporated into the audit report. We provide a copy of the draft report for review prior to finalization. As part of reporting and engagement completion, we will work with management to ensure that data is returned and/or destroyed to comply with the City's expectations around data retention.

Throughout the course of each project, our professionals evaluate the risks associated with each relevant process area to the appropriate layers of information technology (key applications, infrastructure and data).

We can present results to the Citizens Audit Advisory Board in public or executive session, and can also support internal audit's communication of results to the Citizens Audit Advisory Board.







## Available Services for Future Engagements

### In Focus: Advisory Services

Weaver's Advisory Services practice is made up of dedicated professionals who focus on helping clients establish governance, manage risk and maintain compliance.

The professionals in our robust **IT Advisory Services** group have extensive experience providing internal audit, cybersecurity and other IT-focused assessments.

<b>IT INTERNAL AUDIT</b>  Assess risk & evaluate internal controls	<b>CYBERSECURITY</b>  Develop, maintain & monitor up-to-date cybersecurity programs	<b>IT COMPLIANCE</b>  HIPAA, PCI, FDICIA, GLBA, CCPA, NIST, ISO 27001 & more
<b>CONSULTING</b>  Organization, strategy, implementation & problem-solving	<b>DIGITAL TRANSFORMATION &amp; AUTOMATION</b>  Find the answers hidden in data you already have	<b>CIO ADVISORY SERVICES</b>  Strategic & organizational guidance
<b>SOX COMPLIANCE</b>  Sarbanes-Oxley Section 404	<b>PCI COMPLIANCE</b>  Comply with credit card security requirements	<b>SOC EXAMINATIONS</b>  SOC 1, 2, & 3 SOC for Cybersecurity SOC for Supply Chain

Weaver's **Risk Advisory Services** professionals are recognized for their breadth and depth of experience in all phases of risk management, from internal control evaluations over individual processes to complete enterprise risk management.

They bring many years of experience performing risk assessments and providing co-sourced and outsourced internal audit services for a wide of variety clients — including numerous government entities.

<b>GOVERNANCE</b>  Risk Assessment & Internal Controls	<b>COMPLIANCE</b>  Program Development, Review & Monitoring, SOX Compliance	<b>RISK</b>  Enterprise, Entity-Level & Process-Level Risk Assessments, Internal Audit
<b>PERFORMANCE</b>  Business Process Analysis & Improvement, Performance Audit, Quality Assurance Review	<b>GOVERNMENT CONSULTING</b>  Strategy, Operations, Technology & Human Resources	<b>ASSET MGMT. CONSULTING</b>  Internal Audit, Compliance, Risk & Management Consulting

## In Focus: CyberSecurity

To support the City's efforts to assess and enhance the effectiveness of its cybersecurity processes, we propose an entire suite of cybersecurity practices. The City's cybersecurity program must provide an ongoing process that assesses risks, identifies threats, creates protections, monitors systems, and enables quick response and recovery. And that cybersecurity process must be embedded into the organization's governance, not just relegated to a corner of the IT department.

With new personnel in the IT function, re-assessing how cybersecurity is managed and understanding risks and coverage areas is important. Boards like Citizens Audit Advisory Board are most interested in cybersecurity risks when reviewing the technology landscape.

---

Weaver's IT Advisory Services team understands that cybersecurity has to be built into your organization from the ground up.

---

We regularly work with organizations to assess systems and processes against a variety of technical and regulatory requirements, and we're well-versed in the standards and control frameworks used by leading organizations to manage compliance with these regulations.

Weaver looks at your IT environment based on organizational practices that go beyond standards and address cybersecurity at the root of what you do. Each assessment is uniquely tailored, and we work with stakeholders to reflect the right perspective whether strategic, tactical or compliance oriented.



### CYBER RISK ASSESSMENTS

Prioritizing cyber risks that impact security and operations and identifying mitigations.



### COMPLIANCE ASSESSMENTS

Evaluating systems and processes, and providing results based on criteria and requirements.



### VULNERABILITY ASSESSMENTS

Identifying technical weaknesses across devices to improve the overall security posture.



### MATURITY ASMT. & ROADMAPS

Defining the current security profile to improve and target the intended goal state for security.



### GAP & READINESS ASSESSMENTS

Facilitating work sessions and reviews to determine next steps for compliance.



### PENETRATION TESTS

Testing systems as an attacker to highlight flaws and misconfigurations in a controlled manner.



### CYBER AUDITS

Auditing cyber management practices against industry norms to quantify risk for stakeholders.



### CYBER DUE DILIGENCE

Providing buy and sell-side analysis and support aligned to M&A strategy.



### SOCIAL ENGINEERING

Simulating fraudulent e-mails to assess human weaknesses in security programs.

## In Focus: Penetration Testing

Weaver's team offers a multi-layer approach to penetration testing to provide a broad coverage of risks against the City, whether they originate from external actors, insiders within the network, or as a result of phishing campaigns and other social engineering efforts. Each layer is defined by specific objectives and procedures, and targeted deliverables to provide the City with actionable findings and recommendations. Based on your need, our team can tailor a plan that includes all or portion of these layers.

### External Penetration Testing

- ▶ **Overview:** This phase will simulate an attack on the City's external network and focus on attempts to gain unauthorized access to external systems. The engagement will identify vulnerabilities (weaknesses) across the external (public facing) devices through manual testing techniques as well as automated tools. Testing includes time-based grey box penetration testing of up to five business days to closely replicate an external malicious actor's perspective while considering budget.
- ▶ **Objective:** To identify and assess security weaknesses across in-scope external assets and attempt to gain unauthorized access to the City's systems, networks and data from the outside.
- ▶ **Procedures:**
  - » Conduct intelligence gathering tests and perform OSINT/reconnaissance.
  - » Validate targeted scope with management based on information gathered through discovery procedures.
  - » Conduct full port scanning on in scope systems to identify available services and open ports.
  - » Attempt to gain access to systems and penetrate the next layer of the network.
  - » Attempt to identify sensitive information (e.g., user credentials, configurations, sensitive customer data, etc.) from the outside.
  - » Attempt to compromise credentials and identify opportunities to escalate privileges.
  - » Perform unauthenticated vulnerability scans on external IPs to assess overall security hygiene.
  - » Analyze vulnerabilities for risk to the environment based on exploitation vectors.
  - » Perform manual/controlled exploitation of vulnerabilities per Rules of Engagement.
  - » Search for additional vulnerabilities and weaknesses post-exploitation.

▶ **Deliverables:**

- » External and Internal Penetration Testing – A single aggregated formal narrative report including the Scope, Methodology, Findings, and Recommendations of our penetration and vulnerability testing.
- » Includes Management Action Plans for remediation of findings

**Internal Penetration Testing**

▶ **Overview:** This project will simulate an attack on the internal network with the objective of identifying and quantifying internal security risks that may impact the integrity and confidentiality of the City's systems and data. Testing includes time-based grey box internal network penetration testing and credentialed vulnerability scanning of up to eight (8) business days from the City's main facility location. Testing includes both manual and automated techniques.

▶ **Objective:** To identify, assess, and exploit security weaknesses across in-scope assets to obtain unauthorized access to systems and data.

▶ **Procedures:**

- » Attempt to compromise credentials and identify opportunities to escalate privileges.
- » Attempts to gain unauthorized access to systems and data.
- » Identify insecure traffic and conduct man-in-the-middle traffic manipulation tests to intercept sensitive data.
- » Test for security misconfigurations, including insecure device/network protocols and default credentials.
- » Perform authenticated vulnerability scanning using a domain administrator credential.
- » Analyze vulnerabilities for risk to the environment based on exploitation vectors.
- » Review scanning results for anomalies and false positives.
- » Analyze vulnerabilities to identify common trends and root causes.
- » Perform manual/controlled exploitation of vulnerabilities per Rules of Engagement.

▶ **Deliverables:**

- » External and Internal Penetration Testing – A single aggregated formal narrative report including the Scope, Methodology, Findings, and Recommendations of our penetration and vulnerability testing.
- » Includes Management Action Plans for remediation of findings.



## Social Engineering

- ▶ **Overview:** This phase will focus on conducting social engineering techniques to assess employee behavior and the effectiveness of security awareness training. In addition to testing user behavior, email system protections will also be evaluated. This phase includes two email campaigns targeting all City user email addresses.
- ▶ **Objective:** To assess security weaknesses in email users based on behavior and training.
- ▶ **Procedures:**
  - » Identify email recipient targets using Open Source Intelligence (OSINT) and confirm the inventory of targeted email addresses with City management to ensure appropriate coverage and authorization to test.
  - » Develop email scenarios using custom messages including links and/or form fields. Each email phishing campaign will be comprised of an agreed upon premise and will be utilized for all intended recipients.
  - » Analyze interactions and notifications to gather statistics and provide trending reports
  - » Analyze results with organization input to determine the effectiveness of security awareness training.
- ▶ **Deliverables:**
  - » A single aggregated formal narrative report including the Scope, Methodology, Findings and Recommendations of our social engineering assessment.

## In Focus: Vulnerability Assessment

Cybersecurity is constantly evolving and impacts an organization from top to bottom, requiring all users to understand their responsibility in securing the organization. Given the dynamic nature of the environment, a focus on cybersecurity often starts with a vulnerability assessment to understand the current posture. Indeed, a plan to enhance once's defense against new threats and actors is not complete without a reliable starting point to build on.



The image below depicts the key components that a holistic cybersecurity program encompasses, including references to a relevant industry accepted framework (National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF).

We use the supplemental informative criteria when assessing the vulnerability management process and provide any recommendations based on benchmarks and expectations derived from those criteria, along with reasonable recommendations. The vulnerability management process is predominantly in the detect function but is supplemented by key inputs and outcomes from other functions. Our approach recognizes that additional process areas are linked and help inform the vulnerability management process.

### Framework

The NIST CSF is one of the most widely adopted frameworks for cybersecurity and serves as the framework for Weaver's IT audit services. As applicable based on the subject matter area, our professionals will evaluate the risks associated with vulnerability management process areas supporting the in-scope assessment areas. We use NIST CSF as the foundation for security operations processes, and we will develop feasible and relevant recommendations for improvement based on industry knowledge we have gained from our experience with other government entities and from evaluating processes in environments similar to that of the City.

Additionally, as a PCI QSA firm that regularly conducts PCI reports on compliance, we are well-versed in considering the application of multiple criteria. We are equipped to evaluate the City's compliance with applicable federal and state regulations, system policies and other applicable policies such as, HIPAA Security Rule, PCI DSS, and various project requirements requiring implementation of frameworks such as NIST 800-171.

We regularly assess systems and processes against a variety of technical and regulatory requirements and are well-versed in the standards and control frameworks used by leading organizations to manage compliance with these regulations, including:

- ▶ NIST CSF
- ▶ NIST SP 800-53
- ▶ NIST 800-171
- ▶ CIS Critical Security Controls
- ▶ MITRE ATT&CK

Weaver will examine the City's IT environment based on organizational practices to go beyond standards and address cybersecurity *at the root* of what the City does. Each assessment is uniquely tailored, and we will work with City stakeholders to ensure that our perspective is calibrated strategically and tactically without sacrificing a focus on compliance.

- ▶ NIST Cybersecurity Framework (NIST-CSF)
- ▶ Center for Internet Security (CIS) Critical Security Controls (CSC)
- ▶ Payment Card Industry Data Security Standard (PCI-DSS)
- ▶ NIST SP 800-53
- ▶ NIST 800-171
- ▶ DoD Cybersecurity Maturity Model Certification (CMMC)
- ▶ ISO 27000 Series (ISO 27001/27002)



## In Focus: IT Vulnerability Management Phases

The IT Vulnerability Management internal audit would be split into three phases:



### 1 Preliminary

First, Weaver will gain an understanding of the program under review, including a preliminary review of documentation and performing planning activities.



#### Upon Award

We will work with the City's Internal Audit personnel to gain an understanding of the scope, timing, and any other considerations that should be applied to the project. This step will allow us to obtain a baseline understanding of the vulnerability assessments completed to date. For this, we will meet with the Internal Audit team to understand expectations fully, and previous relevant work, inspect available documentation, and discuss known and tracked risks.

Documentation requests at this point may include:

- ▶ Current Organization Charts (for related security functions)
- ▶ Current IT/Security policies and procedures related to Vulnerability Assessments
- ▶ Recent IT audit findings or IT PoAM (Plan of Actions and Milestones) related to governance and the status of prior findings
- ▶ Recent security incidents related to vulnerabilities
- ▶ Current inventory of platforms, tools, and technology utilized in collecting vulnerability scan data
- ▶ Latest vulnerability scan output
- ▶ Technology Project/Initiatives Listing

If there is time between award and contracting, Weaver will utilize that time to perform preliminary planning for coordination with City personnel based on planned/requested timelines. Weaver—in conjunction with Internal Audit—would plan to identify the key stakeholders during this period so that appropriate personnel and teams can be included in the kickoff meeting. And that initial documentation can be provided so that once the kick-off meeting occurs, the project can initiate smoothly.

### Upon Contracting

Once the final scope of work is agreed to and a signed contract is executed, we will coordinate with Internal Audit to set up the kickoff meeting with key personnel. Once signed, we would also prepare the Vulnerability Management internal audit materials that will be utilized to document our procedures and results.

### Kickoff Meeting

We will hold a formal kickoff meeting with key stakeholders to introduce the scope, approach, timeline, and expectations of the participants. We will also discuss the scope of these procedures and the evidence/documents that we will utilize to maximize time with process owners. We will also discuss the areas that are not in the scope of the IT Vulnerability Assessment procedures to ensure that there is alignment on scope.

## 2 Fieldwork

Weaver will conduct a substantive review/analysis of documentation to evaluate the design and effectiveness of internal controls to mitigate the inherent risks and adequacy of the internal controls to mitigate and/or reduce the risk. We'll perform fieldwork remotely or on-site, as agreed upon.



### Evidence Review and Testing

This phase involves working with key personnel to gather all relevant artifacts that demonstrates the controls in place and key capabilities as it relates to vulnerability management. The analysis of gathered documentation will serve as an input to our walkthrough sessions to ensure interviews target more focused questions to build upon knowledge gained during the evidence review phase.

Our review of the Vulnerability Management Program and related policies and procedures will focus on verifying that roles and responsibilities are defined for varying types of data collection methods and are documented in a clear, concise manner to serve as an actionable resource for all phases of detecting, investigating, triaging, remediating, and reporting throughout the vulnerability management lifecycle. We will also verify that criteria were defined in creation of the program and that applicable regulations were considered. Additionally, samples of recent vulnerability scans may be selected (pending available populations) to verify that reports and output were accurately scoped, authenticated (if applicable) and followed documented management processes.

### Walkthroughs and Interviews

Our audit approach involves working with key personnel to thoroughly understand the defined roles, responsibilities and practices in place related to incident response. Through interviews over defined discussion topics, our primary goal is to identify risks associated with the current vulnerability management and related processes to ensure recommendations will enhance the

City's ability to identify, prioritize and remediate vulnerabilities within the environment.

### Additional Procedures

- ▶ Review relevant policies, procedures, and programs in their current state — including but not limited to — the organization's vulnerability management program, and documentation related to scanning, scope reconciliation, remediation, patching, configuration security, and continuous monitoring/reporting of vulnerability trends to management.
- ▶ Conduct interviews/walkthroughs with key personnel to understand internal vulnerability management related practices, scanning procedures, remediation, and approach for reporting the overall health of the vulnerability management process to the Citizens Audit Advisory Board.
- ▶ Review and inspect settings, output, and artifacts related to the following:
  - » Evidence to verify scanning tools utilized, credential configurations, scope of internal scanning, and frequency of performed scanning.
  - » Output from the three most recent internal vulnerability scans conducted within the environment and analyze vulnerabilities to identify trends and root causes.
  - » Documentation related to on-going remediation efforts within the environment and tracking of scan results.
  - » Documentation on the desired state of the vulnerability management program and associated approved management action plans/projects as it relates to the vulnerability management.
  - » Example board materials summarizing internal vulnerability results and trend analysis.

We will continue to request key pieces of information as part of this phase in order to validate the information obtained. Among others, we may request documentation for the following areas:

- ▶ Alignment between IT and additional departments
- ▶ Future state documents or roadmaps of planned initiatives

## 3 Reporting

During the Reporting phase, Weaver will draft a final audit deliverable that will include an executive summary, scope and results.

### Preparation of Draft Results

To document the results of our audit, Weaver will prepare a deliverable that will not only provide a clear, big-picture summary of the assessment, but also address the background, detailed scope and specific methodology of the audit and include identified observations. We will outline risks or deficiencies, and suggest practical, implementable improvements for the City's vulnerability management approach. Our goal is to communicate identified issues early and frequently throughout the audit to ensure risks are socialized prior to the issuing of the full report.

After performing complete quality control reviews of deliverables, our team will provide draft deliverables to Internal Audit for comments and response. We will review and incorporate (as applicable) feedback from Internal Audit, as well as responses and action plans before issuing the final documents. Additionally, an executive-level summary will be created to summarize the scope and objectives as well as the key takeaways from the audit based on Internal Audit's format. This report will be submitted in the format agreed upon with Internal Audit and will document the scope, procedures executed, observations and recommendations for improvement. Our recommendations are intended to strengthen your control structure and to improve effectiveness and operating efficiency.

Weaver regularly produces internal audit reports and will tailor reports based upon the internal organization reporting requirements as well as the unique nature of the subject matter (vulnerability management). Additionally, Weaver has developed executive-level resources in this subject area that can be appended to deliverables to incorporate key attributes and considerations related to vulnerability management and the associated criteria. We will gladly work with Internal Audit to customize the format to best meet the needs of the City.

### **Sharing of Formal Results and Presentation of Formal Assessment**

Our formal results will be provided to City management for a final review. Any remaining questions will be addressed and any final corrections will be made prior to finalizing.



Where there are any areas of interest that are not covered in the scope of the vulnerability management process, we will continuously communicate in status meetings areas that may require additional procedures in the future.

### **Vulnerability Assessment Process Knowledge Transfer**

We welcome the continued participation of Internal Audit personnel in our fieldwork meetings to gain knowledge of IT processes. Based on the results of our IT Vulnerability Management internal audit procedures, we will plan a debrief meeting with the City's Internal Audit team members who supported the project and management personnel to discuss the approach utilized to understand the artifacts and how to monitor the results.

As part of the Vulnerability Management process knowledge transfer, we will plan to generate a process flow to depict the flow of inputs and the output. The process flow and knowledge transfer will be available to those with IT and IT risk knowledge to utilize on a go-forward basis.

## IT Vulnerability Assessment Process





## In Focus: Cloud Services

Cloud services are becoming ubiquitous and transparent to end-users who don't know, and more importantly don't need to know, whether the application they're using is hosted in a data center in the building, across the city, or in a different state altogether. For the IT function however, the introduction of cloud services presents a paradigm shift. From managing all layers of a system, the arrival of cloud services introduces the need to share responsibilities over managing the system with its vendor.

At Weaver, we have developed a suite of services to help adapt your policies and governance standards for the new paradigm, monitor and assess the performance and compliance of your vendors, and design and implement new controls to address the risks and practices unique to the use of the cloud.



## In Focus: IT Risk Assessment

Weaver's IT risk assessment process is designed to gather candid input on organizational risks related to your technology environment. Such risks could impact the organization's ability to

- Deliver services efficiently and effectively to Doral residents
- Protect confidential data and interests of residents
- Comply with regulations or contractual obligations

Our IT risk assessments consider the risk scenarios contained within one of several frameworks such as the Control Objectives for Information and Related Technologies (COBIT), while prioritizing requirements specific to you. In line with information gathered as part of the IT risk assessment, we will evaluate the maturity of the IT environment for each of the subject areas. This allows the City to understand the current state of the IT environment and the current assessed level of risk with the various subject areas.

## Framework & Benchmarking Basis

One of the most widely adopted frameworks for IT risk management, governance and IT auditing, COBIT 2019 serves as the framework for Weaver's IT audit services. As applicable based on the subject matter area, our professionals will evaluate the risks associated with relevant COBIT process areas to the appropriate layers of information technology (key apps, infrastructure, data) supporting the in-scope assessment areas. We use COBIT as the benchmark for IT operations, and we develop feasible and relevant recommendations for improvement based on best practice knowledge gained from our experience at a wide range of government entities ranging from cities such as Doral to some of the largest agencies in the largest states.

In line with the COBIT 2019 Design Guide, the following risk categories map to the COBIT 2019 objectives above and help evaluate the risk profile of an organization. These risk categories are typically evaluated as part of the risk assessment:

- IT-investment decision making, portfolio definition and maintenance
- Program and projects lifecycle management
- IT cost and oversight
- IT expertise, skills, and behavior
- Enterprise/IT architecture
- IT operational infrastructure incidents
- Unauthorized actions
- Software adoption/ usage problems
- Hardware incidents
- Software failures
- Logical attacks (hacking, malware, etc.)
- Third-party/supplier incidents
- Noncompliance
- Geopolitical issues
- Industrial action
- Acts of nature

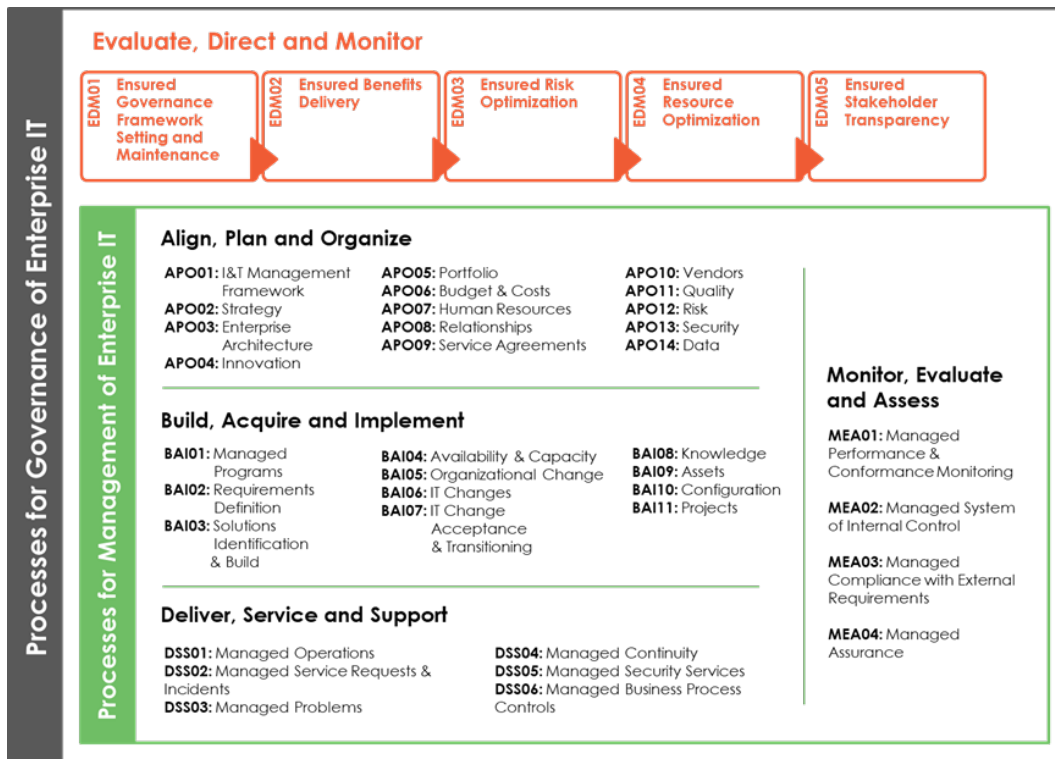
- Technology-based innovation
- Environmental
- Data and information management

Our risk assessment process includes risk identification, applying a risk rating, risk mitigations, and output risk reports.

## Additional Frameworks

Besides NIST CSF, we are experienced in assessing IT environments or their components across multiple frameworks. Additional frameworks allow the City to assess specific practices according to a specialized framework, or to gain a higher degree of confidence over the City's IT practices. Frameworks we frequently rely upon in addition to NIST CSF include:

- The Cloud Security Alliance's (CSA) Cloud Security Controls (CSC); the CSA CSC provide detailed and modular coverage across all the activities that are impacted by an entity's use of cloud-based services, from defining cloud-specific policies, to managing acquisition and oversight of the service, to monitoring the activities that the user entity is responsible for in its consumption of cloud-based services.
- ISACA's Control Objectives for Information Technologies (COBIT); COBIT is one of the most widely adopted frameworks for IT governance, risk management and IT auditing. COBIT domains and objectives include a focus on the identification and management of security programs, requirements definition, stakeholders' participation, vendors management and monitoring of effectiveness, and provide a complete framework for the management of IT Security beyond purely operational procedures.



## In Focus: Government Consulting Services

Combining extensive government advisory experience with innovative technology tools, our dedicated **Government Consulting Services (GCS)** professionals are strategically positioned to assist with opportunities to invest in the future.

In these high-visibility environments, executing large-scale change requires fresh approaches and effective ways to manage risk and report results. Not only does the federal government demand better reporting from states and municipalities, but citizens also want more transparency and accountability. They want to know **how**, **when** and **where** their tax dollars are being put to work for them.

When **efficiency**, **transparency** and **accountability** matter, Weaver's GCS team delivers the results you need.

Our results-oriented approach supports organizations undergoing transformational financial change and modernizing practices in IT, human resources, governance and other areas. From capital projects and economic development initiatives to disaster recovery readiness and ESG goals, Weaver implements innovative tools to help clients attain operational excellence.

### THE FOUR PILLARS OF WEAVER'S GCS





data such as Personally Identifiable Information (PII) or data subject to the Health Insurance Portability and Accountability Act (HIPAA).

During the Planning phase of the engagement, Weaver and the City will discuss the sensitivity of the data that may be accessed during the engagement. Jointly, we will clearly delineate the scope of the engagements, including the systems and data stores in scope. In requesting evidence from City personnel, Weaver will design its requests to specifically target the relevant systems and data stores to reduce the risks that unintended data may be provided as a response. Weaver will also discuss with City personnel appropriate communication channels to restrict exposure to unauthorized parties, such as the use of encrypted emails or reliance on a secure, authenticated portal to exchange data between the City and Weaver.

If the need arises at any time during the engagement, Weaver can call upon its in-house Forensics and Litigation Services team to ensure data is handled and retained in such a way as to be able to demonstrate integrity and chain-of-custody.

To further isolate and remediate potential risks, we work to thoroughly understand engagement criteria, including applicable regulatory and agency requirements. This enables us to detail specific procedures that map to defined outcomes, with any deviations carefully considered when determining the final results of each engagement.

Weaver incorporates these specific engagement-level and firm-level quality programs to evaluate the effectiveness of our team's procedures on each engagement.

### **Engagement Quality**

From seasoned partners to the newest associates, all Weaver professionals understand that our commitment to quality requires thoughtful planning, consistent follow-through and attention to detail.

We start by ensuring that staff have the knowledge and experience required to carry out their responsibilities. Recognizing that supervisors and other reviewers can complement that knowledge, our policies and procedures also provide for consultation on significant matters and multiple layers of technical review.

---

Your engagement partner and their team will work closely together to ensure effective planning, and will provide multiple levels of quality review.

---



Automated error-checking tools are used when appropriate, but we never consider them a substitute for the thoughtful management review and oversight needed to deliver the highest quality work possible. During planning, we work with you to properly define performance standards, including the overall goals, schedule, staffing requirements (in number and experience/skills required) and deliverable requirements.

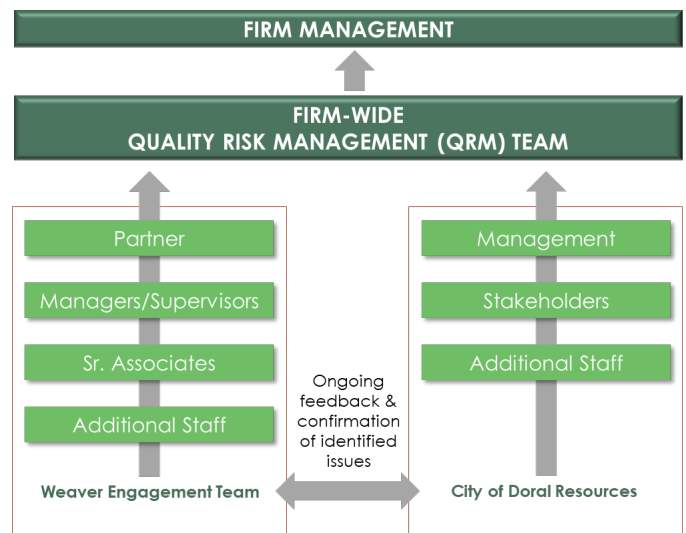
At end of the engagement, we hold an exit conference to discuss results, including any findings and observations. We'll also discuss what went well or what could be changed, so we can incorporate that knowledge into our future delivery of services.

**Firmwide Quality**

Weaver has created and adheres to a System of Quality Management (SOQM) Document that demands integrity, objectivity, competence and diligence from our professionals in all engagements, whatever their nature.

We demand independence in fact and appearance in engagements where independence is required by applicable laws, regulations or requirements of professional societies. We take steps to ensure that personnel assigned to engagements have the professional and specialized knowledge required to carry out their responsibilities, recognizing that supervisors, other reviewers and consultants can complement that knowledge.

These quality control guidelines mandate that our engagement teams retain sufficient evidence to substantiate the procedures we performed on the engagement. Such work papers are retained for a minimum of three years, at the firm's expense. As a matter of practice, we offer to make a copy of all work papers available to clients.



Our SOQM defines the philosophy of our practice and our commitment to service excellence. More specifically, to achieve high-quality professional performance, Weaver has adopted policies and procedures that implement the quality control standards established by the AICPA.



Our Quality and Risk Management Committee oversees the firm's performance regarding quality control. In addition, Weaver's successful performance in external peer reviews, conducted every three years, further demonstrates the effectiveness of our quality assurance efforts. Due to the confidential nature and size of Weaver's SOQM, we do not provide a copy of the document as part of our proposals.

d. Reporting: An overview of how progress will be reported, communication channels, and how feedback and issues will be addressed throughout the audit process.

## Frequent and Open Communication

Throughout each engagement, and our entire relationship with you, Weaver will communicate openly and often. Your Weaver team will hold the following meetings with management and, when appropriate, with those charged with governance:

- ▶ A planning meeting to discuss any prior services and learn your expectations for the upcoming engagement
- ▶ Entrance and exit conferences
- ▶ Progress conferences during the audit to discuss work in progress and open items
- ▶ Presentations of the final report/s and other required deliverables

We'll use these communications to:

- ▶ Provide technical updates and discuss the impact on your organization
- ▶ Learn about changes in your forward-looking strategies or needs
- ▶ Understand your overall satisfaction to date

We'll keep you informed of any significant events that arise during the engagement. Whenever there's a question or a potential issue, we'll bring it to your attention, seek your confirmation of the data and ask about any relevant circumstances; we encourage you to do the same.

---

Through open communication, our objective is to eliminate surprises while providing an efficient, effective engagement.



---

## Project Management

Creating value in any engagement starts with open and regular communication, including hands-on involvement of the partners and team leadership, all of whom will communicate with you on a regular basis.

This serves as the foundation of every Weaver engagement.

In addition to tailoring our teams to each specific engagement, your partner will remain actively engaged to ensure adherence to the budget and timeline, as well as quality standards.

The team will monitor progress daily to ensure that work is proceeding on schedule and budget, and is meeting established performance standards.

**Reema Parappilly** will operate as the relationship partner with City of Doral on any internal audit related requests and utilize **Trip Hillman** as the cybersecurity partner to support the specialized projects that require cybersecurity knowledge.



**SOLICITATION RESPONSE FORM**

**City of Doral ITN No. 2024-05  
Independent IT Audit Services**

Date Submitted	March 27, 2024
Company Legal Name	Weaver and Tidwell, L.L.P.
Date of Entity Formation	1950
Entity Type (select one)	Limited Liability Partnership
Corporate Address	2821 W 7th St, Ste 700; Ft. Worth, TX 76107
Office Location	4400 Post Oak Parkway, Suite1100; Houston, TX 77027
Taxpayer Identification No.	75-0786316
Authorized Representative (Name and Title)	Reema Parappilly, Partner, IT Advisory Services

1. The undersigned Bidder/Proposer agrees, if this Bid is accepted by the City, to enter into an agreement with the City of Doral to perform and furnish all goods and/or services as specified or indicated in the Contract for the Price and within the timeframe indicated in this proposal and in accordance with the terms and conditions of the Contract.
2. Bidder/Proposer accepts all of the terms and conditions of the Solicitation, including without limitation those dealing with the disposition of Bid Security. This Bid will remain subject to acceptance for 180 days after the day of Bid opening. Bidder/Proposer agrees to sign and submit the Contract with any applicable documents required by this ITN within ten days after the date of City’s Notice of Award (If applicable).
3. By responding to this sealed Solicitation, the Bidder/Proposer makes all representations required by the Solicitation and further warrants and represents that Bidder/Proposer acknowledges that it has received and examined copies of the entire Solicitation documents including all of the following addenda:  
 Addendum No.: 1 Dated: 3/25/24 Addendum No.: \_\_\_\_\_ Dated: \_\_\_\_\_  
 Addendum No.: 2 Dated: 04/01/24 Addendum No.: \_\_\_\_\_ Dated: \_\_\_\_\_  
 Check here If no Addenda were issued by the City.
4. Bidder/Proposer further warrants and represents that it has familiarized themselves with the nature and extent of the Contract, required goods and/or services, site, locality, and all local conditions and applicable laws and regulations that in any manner may affect cost, progress, performance, or furnishing of the Work.
5. Bidder/Proposer further warrants and represents that it has studied carefully all documentation and information provided to the extent applicable to the Work, and has obtained and carefully studied (or assumes responsibility for obtaining and carefully studying) all information provided that pertains to the project or otherwise may affect the cost, progress, performance, or furnishing of the Work, and no additional examinations, investigations, explorations, tests, reports or similar information or data are or will be required by Bidder/Proposer for such purposes.

6. Bidder/Proposer further warrants and represents that it has given the City written notice of all errors or discrepancies it has discovered in the Contract and the resolution thereof by the City is acceptable to Bidder/Proposer.
7. Bidder/Proposer further warrants and represents that this Bid/Proposal is genuine and not made in the interest of or on behalf of any other undisclosed person, firm or corporation; Bidder/Proposer has not directly or indirectly induced or solicited any other Bidder/Proposer to submit a false or sham Proposal; Bidder/Proposer has not solicited or induced any person, firm or corporation to refrain from submitting; and Bidder/Proposer has not sought by collusion to obtain for itself any advantage over any other Bidder/Proposer or over the City.
8. Bidder/Proposer understands that the quantities provided are only provided for proposal evaluation only. The actual quantities may be higher or lower than those in the proposal form.
9. Bidder/Proposer understands and agrees that the Contract Price is Unit Rate Contract to furnish and deliver all of the Work complete in place as such the Proposer shall furnish all labor, materials, equipment, tools superintendence, and services necessary to provide a complete Project.
10. Communications concerning this Proposal shall be addressed to:


Bidder/Proposer: Weaver and Tidwell, L.L.P.  
Telephone: 832.320.3254  
Email Address: reema.p@weaver.com  
Attention: Reema Parappilly, Partner, IT Advisory Services

11. The terms used in this response which are defined in the above-referenced Solicitation shall have the meanings assigned to them in such Solicitation.

**STATEMENT**

I understand that a "person" as defined in 287.133(1)(e), Florida Statutes, means any natural person or entity organized under the laws of any state or of the United States with the legal power to enter into a binding Contract and which Bids or applies to Bid on Contracts for the provision of goods or services let by a public entity, or which otherwise transacts or applies to transact business with a public entity. The term "persons" includes officers, directors, executives, partners, shareholders, employees, members, and agents active in management of the entity.

SUBMITTED THIS 27th DAY OF March, 2024.

Company Name: Weaver and Tidwell, L.L.P.  
Company Address: 4400 Post Oak Parkway, Suite1100; Houston, TX 77027  
Authorized Representative Signature: 

**PROPOSER QUALIFICATION STATEMENT**

The Proposer's response to this questionnaire will be utilized as part of the City's evaluation to ensure that the Proposer meets, to the satisfaction of the City, the minimum requirements for participating in this Solicitation.

**PROPOSER MUST PROVIDE DETAILS FULFILLING THE SOLICITATION'S MINIMUM EXPERIENCE REQUIREMENTS IN THE FORM BELOW. IT IS MANDATORY THAT PROPOSERS USE THIS FORM IN ORDER TO INDICATE THAT THE MINIMUM EXPERIENCE REQUIREMENT IS MET. NO EXCEPTIONS WILL BE MADE.**

Proposer	Weaver and Tidwell, L.L.P.		
Years in Business	74		
Years of Experience Providing Independent IT Audit Services	19		
<b>Project No. 1</b>			
Project Name:	Various: See below.		
Project Description:	Weaver has long provided advisory services to Dallas: financial and IT controls work as well as internal control reviews and evaluation. We've performed internal audits over Body Worn and In-Car Cameras; Computer Incident Response Management; and Backup Maintenance Internal Audits		
Budget/Cost:	IT Audit Only: \$32,000	Contract Dates:	2009-15; 2020 - Present
Owner/Client Name:	City of Dallas	Reference Name:	Mark Swann
Reference Phone No.:	214.670.3222	Reference Email:	mark.swann@dallascityhall.com
<b>Project No. 2</b>			
Project Name:	IT Vulnerability Assessment & Security Consulting		
Project Description:	Weaver conducted a technical assessment of the vulnerabilities and weaknesses of a web application. The audit included a detailed analysis of the application's security controls, access management protocols and vulnerability management processes.		
Budget/Cost:	\$100,000	Contract Dates:	2021; 2023
Owner/Client Name:	City of Austin - Water	Reference Name:	Sharyn Leyendecker. IT Security Consultant
Reference Phone No.:	512.972.0139	Reference Email:	sharyn.leyendecker@austintexas.gov
<b>Project No. 3</b>			
Project Name:	Internal Audit		
Project Description:	Weaver is performing a CIS Critical Security Controls version 8 based cybersecurity maturity assessment to determine if key cybersecurity functions are performed and if they are conducted at a consistently level across the environment. Weaver's also performed an assessment of the Master Credit Facility Program implemented within the Real Estate Investments function.		
Budget/Cost:	\$55,349	Contract Dates:	2023 - Present
Owner/Client Name:	State Board of Admin. of Florida	Reference Name:	Kim Stirner, Chief Audit Exec. & I.G.
Reference Phone No.:	850.413.1244	Reference Email:	kimberly.stirner@sbafla.com

**BIDDER/PROPOSER AFFIDAVITS**

**Business Name:** Weaver and Tidwell, L.L.P.

D.B.A.: \_\_\_\_\_ Federal I.D. No.: 75-0786316

Business Address: 2821 W 7th St, Ste 700

City: Forth Worth State: Texas Zip: 76107

I, the undersigned affiant do swear and affirm that I am an authorized agent of the above-named business (“Bidder”) and authorized to make the following statements and certifications on Bidder’s behalf:

**1. Ownership Disclosure**

Pursuant to City Code Section 2-384, the above-named Bidder hereby discloses the following principals, individuals, or companies with five percent (5%) or greater ownership interest in Bidder (supplement as needed):

<i>Name</i>	<i>Address</i>	<i>% Ownership</i>
John Mackel	4400 Post Oak Parkway, Suite 1100 Houston, TX 77027	7.62
Alyssa Martin	2300 N. Field Street, Suite 1000 Dallas, TX 75201	5.11
Sean Muller	4400 Post Oak Parkway, Suite 1100 Houston, TX 77027	5.11
David Rook	4400 Post Oak Parkway, Suite 1100 Houston, TX 77027	5.87
Wade Watson	4400 Post Oak Parkway, Suite 1100 Houston, TX 77027	5.25

The above-named Bidder hereby discloses the following subcontractors (supplement as needed):

<i>Name</i>	<i>Address</i>	
Gradient Solutions	Mansfield, TX 76063	

Bidder hereby recognizes and certifies that no elected official, board member, or employee of the City of Doral (“City”) shall have a financial interest in any transactions or any compensation to be paid under or through any transactions between Bidder and City, and further, that no City employee, nor any elected or appointed officer (including City board members) of the City, nor any spouse, parent or child of such employee or elected or appointed officer of the City, may be a partner, officer, director or proprietor of Bidder, and further, that no such City employee or elected or appointed officer, or the spouse, parent or child of any of them, alone or in combination, may have a material interest in the Bidder. Material interest means direct or indirect ownership of more than 5% of the total assets or capital stock of the Bidder.

Any exception to these above-described restrictions must be expressly provided by applicable law or ordinance and be confirmed in writing by City. Further, Bidder recognizes that with respect to any transactions between Bidder and City, if any Bidder violates or is a party to a violation of the ethics ordinances or rules of the City, the provisions of Miami-Dade County Code Section 2-11.1, as applicable to City, or the provisions of Chapter 112, part III, Fla. Stat., the Code of Ethics for Public Officers and Employees, such Bidder may be disqualified from furnishing the goods or services for which the bid or proposal is submitted and may be further disqualified from submitting any future bids or

proposals for goods or services to City. The term "Bidder," as used herein, include any person or entity making a proposal herein to City or providing goods or services to City.

## 2. Public Entity Crimes

1. Bidder is familiar with and understands the provisions of Section 287.133, Florida Statutes
2. Bidder further understands that a person or affiliate who has been placed on the convicted Bidder list following a conviction for a public entity crime may not submit a bid, proposal, or reply on a contract to provide any goods or services to a public entity; may not submit a bid, proposal, or reply on a contract with a public entity for the construction or repair of a public building or public work; may not submit bids, proposals, or replies on leases of real property to a public entity; may not be awarded or perform work as a contractor, supplier, subcontractor, or consultant under a contract with any public entity; and may not transact business with any public entity in excess of the threshold amount provided in s. 287.017 for CATEGORY TWO for a period of 36 months following the date of being placed on the convicted Bidder list.
3. Based on information and belief, the statement which I have marked below is true in relation to the entity submitting this sworn statement. (INDICATE WHICH STATEMENT APPLIES.)
  - Neither the entity submitting this sworn statement, nor any of its officers, directors, executives, partners, shareholders, employees, members, or agents who are active in the management of the entity, nor any affiliate of the entity has been charged with and convicted of a public entity crime subsequent to July 1, 1989.
  - \_\_\_\_\_ The entity submitting this sworn statement, or one or more of its officers, directors, executives, partners, shareholders, employees, members, or agents who are active in the management of the entity, or an affiliate of the entity has been charged with and convicted of a public entity crime subsequent to July 1, 1989.
  - \_\_\_\_\_ The entity submitting this sworn statement, or one or more of its officers, directors, executives, partners, shareholders, employees, members, or agents who are active in the management of the entity, or an affiliate of the entity has been charged with and convicted of a public entity crime subsequent to July 1, 1989. However, there has been a subsequent proceeding before a Hearing Officer of the State of Florida, Division of Administrative Hearings and the Final Order entered by the Hearing Officer of the State of Florida, Division of Administrative Hearings and the Final Order entered by the Hearing Officer determined that it was not in the public interest to place the entity submitting this sworn statement on the convicted Bidder list. (Attach a copy of the final order.)

## 3. Compliance With Foreign Entity Laws

Applicant certifies as follows:

- a. Bidder is not owned by the government of a foreign country of concern, as defined in Section 287.138, Florida Statutes.
- b. The government of a foreign country of concern does not have a controlling interest in Bidder, as defined in Section 287.138, Florida Statutes.
- c. Bidder is not organized under the laws of a foreign country of concern, as defined in Section 287.138, Florida Statutes.
- d. Bidder does not have a principal place of business in a foreign country of concern, as defined in Section 287.138, Florida Statutes.
- e. Bidder is not on the Scrutinized Companies with Activities in Sudan List or the Scrutinized Companies with Activities in Iran Terrorism Sectors List, created pursuant to s. 215.473.
- f. Bidder is not engaged in business operations in Cuba or Syria.
- g. Bidder is not participating in a boycott of Israel, and is not on the Scrutinized Companies that Boycott Israel list in accordance with the requirements of Sections 287.135 and F.S. 215.473, Florida Statutes

#### **4. Disability, Nondiscrimination, and Equal Employment Opportunity**

Applicant certifies that Bidder is in compliance with and agrees to continue to comply with, and ensure that any subcontractor, or third party contractor under any and all contracts with the City of Doral complies with all applicable requirements of the laws listed below including, but not limited to, those provisions pertaining to employment, provision of programs and services, transportation, communications, access to facilities, renovations, and new construction.

- The American with Disabilities Act of 1990 (ADA), Pub. L. 101-336, 104 Stat 327, 42 USC 1210112213 and 47 USC Sections 225 and 661 including Title I, Employment; Title II, Public Services; Title III, Public Accommodations and Services Operated by Private entities; Title IV, Telecommunications; and Title V, Miscellaneous Provisions.
- The Florida Americans with Disabilities Accessibility Implementation Act of 1993, Section 553.501 553.513, Florida Statutes.
- The Rehabilitation Act of 1973, 229 USC Section 794.
- The Federal Transit Act, as amended 49 USC Section 1612.
- The Fair Housing Act as amended 42 USC Section 3601-3631

#### **5. Conformance with OSHA Standards**

Applicant certifies and agrees that Applicant has the sole responsibility for compliance with all the requirements of the Federal Occupational Safety and Health Act of 1970, and all State and local safety and health regulations, and in the event the City engages Bidder, Bidder agrees to indemnify and hold harmless the City of Doral, against any and all liability, claims, damages losses and expenses the City may incur due to the failure of itself or any of its subcontractors to comply with such act or regulation in the performance of the contract.

#### **6. E-Verify Program Affidavit**

Affiant certifies the following:

- a. Affiant is familiar with and understands the provisions of Section 448.095, Florida Statutes and 48 CFR 52.222-54 and has sufficient knowledge of the personnel practices of the Bidder to execute this Declaration on behalf of the Bidder.
- b. Bidder has registered with and utilizes the federal work authorization program commonly known as E-Verify or any subsequent replacement program, in accordance with the applicable provisions and deadlines established in F.S. 448.095, which prohibits the employment, contracting or sub-contracting with an unauthorized alien.
- c. Bidder does not knowingly employ Affiants or retain in its employ a person whose immigration status makes them ineligible to work for the Bidder.
- d. Bidder has verified that any subcontractors utilized to deliver goods or services to the City through the Contractor's contract with the City use the E-Verify system and do not knowingly employ persons whose immigration status makes them ineligible to work for the subcontractor. The undersigned further confirms that it has obtained all necessary affidavits from its subcontractors, if applicable, in compliance with F.S. 448.095, and that such affidavits shall be provided to the City upon request.
- e. Failure to comply with the requirements of F.S. 448.095 may result in termination of the Bidder's contract(s) with the City of Doral.

#### **7. No Contingency Affidavit**

Affiant certifies the following:

- a. Neither Bidder nor any principal, employee, agent, representative or family member has promised to pay, and

Bidder has not and will not pay, a fee the amount of which is contingent upon the City of Doral awarding a contract.

- b. Bidder warrants that neither it, nor any principal, employee, agent, or representative has procured, or attempted to procure, a contract with the City of Doral in violation of any of the provisions of the Miami- Dade County conflict of interest and code of ethics ordinances.
- c. Bidder acknowledges that a violation of this warranty may result in the termination of any contracts and forfeiture of funds paid, or to be paid, to the Bidder if awarded a contract.

#### **8. Copeland Anti-Kickback Affidavit**

Affiant certifies that no portion of any sums will be paid to any employees of the City of Doral, its elected officials, or its consultants, as a commission, kickback, reward or gift, directly or indirectly by Bidder or any member of Bidder's firm or by any officer of the corporation in exchange for business with the City of Doral.

#### **9. Non-Collusion Affidavit**

I, the undersigned affiant, swear or affirm that:

- a. Affiant is fully informed respecting the preparation and contents of the attached Bid/Proposal by Contractor and of all pertinent circumstances respecting such Bid/Proposal.
- b. Such Bid/Proposal is genuine and is not a collusive or sham Bid/Proposal.
- c. Neither the said Contractor nor any of its officers, partners, owners, agents, representatives, employees or parties in interest, including Affiant, have in any way colluded, conspired, connived or agreed, directly or indirectly, with any other firm or person to submit a collusive or sham Bid/Proposal in connection with the Work for which the attached Bid/Proposal has been submitted; or to refrain from bidding in connection with such Work; or have in any manner, directly or indirectly, sought by agreement or collusion, or communication, or conference with any firm or person to fix any overhead, profit, or cost elements of the Bid/Proposal or of any other person submitting a response to the solicitation, or to fix any overhead, profit, or cost elements of the quoted price(s) or the quoted price(s) of any other bidding/proposing person, or to secure through any collusion, conspiracy, connivance, or unlawful agreement any advantage against the City or any person interested in the proposed Work.
- d. The price(s) quoted in the attached Bid/Proposal are fair and proper and are not tainted by any collusion, conspiracy, connivance, or unlawful agreement on the part of the Contractor or any other of its agents, representatives, owners, employees or parties in interest, including this Affiant.

#### **10. Drug Free Workplace Program**

Bidder, in accordance with Florida statute 287.087 hereby certifies that the Bidder does all of the following:

- a. Publishes a statement notifying employees that the unlawful manufacture, distribution, dispensing, possession, or use of a controlled substance is prohibited in the workplace and specifying the actions that will be taken against employees for violations of such prohibition.
- b. Informs Employees about the dangers of drug abuse in the workplace, the business' policy of maintaining drug-free workplace, any available drug counseling, rehabilitation, and employee assistance programs, and the penalties that may be imposed upon employees for drug abuse violations.
- c. Gives each employee engaged in providing the commodities or contractual services that are under bid a copy of the statement specified in subsection (a).
- d. In the statement specified in subsection (a), notifies the employees that, as a conditions of working on the commodities or contractual services that are under bid, the employee will abide by the terms of the statement and will notify the employer of any conviction of, or plea of guilty or nolo contendere to, any violation of chapter 893 or of any controlled substance law of the United States or any state, for a violation occurring in the workplace no later than five (5) days after such conviction.

- e. Imposes a sanction on, or require the satisfactory participation in, a drug abuse assistance or rehabilitation program if such is available in the employee’s community, by any employee who is so convicted.
- f. Makes a good faith effort to continue to maintain a drug-free workplace through implementation of this section.

Select here if Not Applicable

**11. Cone of Silence Certification**

Affiant certifies and that Affiant has read and understands the Cone of Silence” requirements set forth in this Solicitation and further certify that neither I, nor any agent or representative of the Company has violated this provision.

**BIDDER AFFIRMATION**

I, the undersigned affiant, being first duly sworn as an authorized agent of the below-named Bidder, does hereby affirm and attest under penalty of perjury as the proposed Bidder for City of Doral that the certifications and statements provided above on behalf of Bidder are true to the best of affiant’s knowledge and belief and that Bidder is compliant with all requirements outlined in these City of Doral Affidavits. Bidder acknowledges it is required to comply with and keep current all statements sworn to in the above affidavits and will notify the City of Doral immediately if any of the statements attested hereto are no longer valid.

Weaver and Tidwell, L.L.P.  
 Bidder Name  
[Signature]  
 Affiant Signature

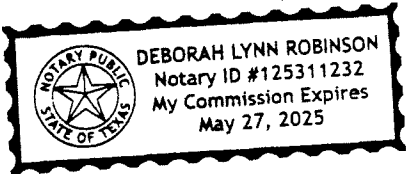
March 26, 2024  
 Date Signed  
 Reema Parappilly, Partner, IT Advisory Services  
 Affiant Name & Title (Printed)

STATE OF Texas  
 COUNTY OF Harris

The foregoing instrument was affirmed, subscribed, and sworn to before me this 26<sup>th</sup> day of March 2024 by means of  physical presence or  online notarization, by Deborah Lynn Robinson who is personally known to me or who produced the following identification: personally known

[Notary Seal]

Deborah Lynn Robinson  
 Notary Public for the State of Texas  
 My commission expires: May 27, 2025





**LEVEL 1 PRINCIPAL’S ADOPTION AGREEMENT**


This Level 1 Principal’s Adoption Agreement is executed and made effective for all purposes as of the 26<sup>th</sup> day of October, 2022, by the undersigned individual and Weaver and Tidwell, L.L.P. (the “Partnership”).

1. The undersigned individual hereby agrees to be subject to, and bound by, at all times, all of the terms and conditions of the Amended and Restated Partnership Agreement of Weaver and Tidwell, L.L.P. (Dated as of October 26, 2022), as the same may be amended from time-to-time, the “Partnership Agreement”). Without limitation of the foregoing, the undersigned individual is deemed to have made all of the representations, warranties, acknowledgments, waivers, covenants and agreements set forth in the Partnership Agreement with respect to Level 1 Principals.


2. The undersigned CEO of the Partnership hereby acknowledges on the behalf of the Partnership the continued status of the undersigned individual as a Level 1 Principal.

IN WITNESS WHEREOF, the parties hereto have caused this Adoption Agreement to be executed as of the date first written above.

**LEVEL 1 PRINCIPAL:**

Signed:   
Printed Name: Reema Parappilly  
Date: 11/08/2022

**WEAVER AND TIDWELL, L.L.P.:**

By:   
Printed Name: John Mackel  
Title: CEO  
Date: 10/26/22

**SIGNATURE CERTIFICATE**




**REFERENCE NUMBER**

F5FC63F7-E2CC-40E8-B7C5-8591204D7FCD

TRANSACTION DETAILS	DOCUMENT DETAILS
<p><b>Reference Number</b> F5FC63F7-E2CC-40E8-B7C5-8591204D7FCD</p> <p><b>Transaction Type</b> Bulk Send</p> <p><b>Sent At</b> 10/31/2022 16:04 EDT</p> <p><b>Executed At</b> 11/08/2022 12:30 EST</p> <p><b>Identity Method</b> email</p> <p><b>Distribution Method</b> email</p> <p><b>Signed Checksum</b> 73a6cfffcd744ba4337c5159a4a865bbe043ded4158e38ab31d1b03a638dcce</p> <p><b>Signer Sequencing</b> Disabled</p> <p><b>Document Passcode</b> Disabled</p>	<p><b>Document Name</b> Exhibit A Level 1 Principal Adoption Agreement</p> <p><b>Filename</b> exhibit_a_level_1_principal_adoption_agreement_.pdf</p> <p><b>Pages</b> 1 page</p> <p><b>Content Type</b> application/pdf</p> <p><b>File Size</b> 69.7 KB</p> <p><b>Original Checksum</b> 4157caa88b60549e4e4233d162058c23c12da0ab8fa49528ec1928cf8905227b</p>

**SIGNERS**

SIGNER	E-SIGNATURE	EVENTS
<p><b>Name</b> Reema Parappilly</p> <p><b>Email</b> reema.p@weaver.com</p> <p><b>Components</b> 3</p>	<p><b>Status</b> signed</p> <p><b>Multi-factor Digital Fingerprint Checksum</b> f0ef2321c72584374686961a9b2e9177432f173978e38fdcad3c2ad32183da23</p> <p><b>IP Address</b> 104.4.61.185</p> <p><b>Device</b> Chrome via Windows</p> <p><b>Drawn Signature</b> </p> <p><b>Signature Reference ID</b> FE52D8C0</p> <p><b>Signature Biometric Count</b> 313</p>	<p><b>Viewed At</b> 11/08/2022 12:30 EST</p> <p><b>Identity Authenticated At</b> 11/08/2022 12:30 EST</p> <p><b>Signed At</b> 11/08/2022 12:30 EST</p>

**AUDITS**

TIMESTAMP	AUDIT
10/31/2022 16:04 EDT	Dana Burris (dana.burris@weaver.com) created document 'exhibit_a_level_1_principal_adoption_agreement_.pdf' on Chrome via Windows from 199.247.32.123.
10/31/2022 16:04 EDT	Reema Parappilly (reema.p@weaver.com) was emailed a link to sign.
11/01/2022 16:43 EDT	Reema Parappilly (reema.p@weaver.com) was emailed a reminder.
11/08/2022 12:30 EST	Reema Parappilly (reema.p@weaver.com) viewed the document on Chrome via Windows from 104.4.61.185.
11/08/2022 12:30 EST	Reema Parappilly (reema.p@weaver.com) viewed the document on Chrome via Windows from 54.85.38.145.
11/08/2022 12:30 EST	Reema Parappilly (reema.p@weaver.com) authenticated via email on Chrome via Windows from

104.4.61.185.

11/08/2022 12:30 EST

Reema Parappilly (reema.p@weaver.com) signed the document on Chrome via Windows from 104.4.61.185.

**CONFLICT OF INTEREST DISCLOSURE**

**Business Name:** Weaver and Tidwell, L.L.P.

D.B.A.: \_\_\_\_\_ Federal I.D. No.: 75-0786316

Business Address: 2821 W 7th St, Ste 700

City: Fort Worth State: Texas Zip: 76107


Please note that all business entities interested in or conducting business with the City are subject to comply with the City of Doral’s conflict of interest policies as stated within the certification section below. If a vendor has a relationship with a City of Doral official or employee, an immediate family member of a City of Doral official or employee, the vendor shall disclose the information required below.

1. No City official or employee or City employee’s immediate family member has an ownership interest in vendor’s company or is deriving personal financial gain from this contract.
2. No retired or separated City official or employee who has been retired or separated from the City for less than one (1) year has an ownership interest in vendor’s Company.
3. No City employee is contemporaneously employed or prospectively to be employed with the vendor.
4. Vendor hereby declares it has not and will not provide gifts or hospitality of any dollar value or any other gratuities to any City employee or elected official to obtain or maintain a contract.

<b>Conflict of Interest Disclosure*</b>	
Name of City of Doral employees, elected officials, or immediate family members with whom there may be a potential conflict of interest:  _____  _____  _____	<input type="checkbox"/> Relationship to employee <input type="checkbox"/> Interest in vendor’s company <input type="checkbox"/> Other (please describe below)  _____  _____  <input checked="" type="checkbox"/> No Conflict of Interest

*\*Disclosing a potential conflict of interest does not automatically disqualify vendors. In the event vendors do not disclose potential conflicts of interest and they are detected by the City, vendor will be exempt from doing business with the City.*

**I certify that this Conflict-of-Interest Disclosure has been examined by me and that its contents are true and correct to my knowledge and belief and I have the authority to so certify on behalf of the Vendor by my signature below:**

	March 27, 2024	Reema Parappilly, Partner, IT Advisory Services
Signature of Authorized Representative	Date	Printed Name of Authorized Representative

**MINIMUM INSURANCE REQUIREMENTS**

**I. Commercial General Liability**

- A. Limits of Liability
  - Each Occurrence \$1,000,000
  - Policy Aggregate (Per job or project) \$1,000,000
- B. Endorsements Required
  - City of Doral listed as an additional insured.
  - Contingent & Contractual Liability
  - Waiver of Subrogation in favor of City

**II. Professional Liability**

- A. Limits of Liability \$1,000,000

**III. Workers Compensation**

Statutory- State of Florida

**Employer’s Liability**

- A. Limits of Liability
    - \$500,000 for bodily injury caused by an accident, each accident.
    - \$500,000 for bodily injury caused by disease, each employee.
    - \$500,000 for bodily injury caused by disease, policy limit.
- Workers Compensation insurance must be provided for all persons fulfilling this contract, whether employed, contracted, temporary or subcontracted.

**IV. Cyber Liability**

- A. Limits of Liability \$5,000,000
- B. Endorsements Required
  - City of Doral listed as an additional insured.
  - Contingent & Contractual Liability
  - Waiver of Subrogation in favor of City

**Subcontractors’ Compliance:** It is the responsibility of the Vendor to ensure that all Subcontractors comply with all insurance requirements.

All above coverage must remain in force and Certificate of Insurance on file with City without interruption for the duration of this agreement. Policies shall provide the City of Doral with 30 days’ written notice of cancellation or material change from the insurer. If the policies do not contain such a provision, it is the responsibility of the Vendor to provide such notice within 10 days of the change or cancellation.

Certificate Holder: City of Doral, Florida  
8401 NW 53<sup>rd</sup> Terrace  
Doral, FL 33166

Certificates/Evidence of Property Insurance forms must confirm insurance provisions required herein. Certificates shall include Agreement, Bid/Contract number, dates, and other identifying references.

Insurance Companies must be authorized to do business in the State of Florida and must be rated no less than “A-” as to management, and no less than “Class V” as to financial strength, by the latest edition of AM Best’s Insurance Guide, or its equivalent.

Coverage and Certificates of Insurance are subject to review and verification by City of Doral Risk Management. City reserves the right but not the obligation to reject any insurer providing coverage due to poor or deteriorating financial condition. The City reserves the right to amend insurance requirements in order to sufficiently address the scope of services. These insurance requirements shall not limit the liability of the Vendor. The City does not represent these types or amounts of insurance to be sufficient or adequate to protect the Vendor/Vendor’s interests or liabilities but are merely minimums.



# CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)

8/14/2023

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

**IMPORTANT:** If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

<b>PRODUCER</b> Edgewood Partners Insurance Center EPIC Brokers 14881 Quorum Drive, Suite 850 DALLAS, TX 75254  www.epicbrokers.com	<b>CONTACT NAME:</b> Yvette Camacho <b>PHONE (A/C, No. Ext):</b> <b>FAX (A/C, No):</b> <b>E-MAIL ADDRESS:</b> yvette.camacho@epicbrokers.com
	<b>INSURER(S) AFFORDING COVERAGE</b> <b>INSURER A:</b> Continental Insurance Company <b>INSURER B:</b> National Fire Insurance Co of Hartford <b>INSURER C:</b> <b>INSURER D:</b> <b>INSURER E:</b> <b>INSURER F:</b>

**COVERAGES**

CERTIFICATE NUMBER: 75751091

REVISION NUMBER:

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	<input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR  GEN'L AGGREGATE LIMIT APPLIES PER: <input checked="" type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input checked="" type="checkbox"/> LOC OTHER:			6081459505	8/15/2023	8/15/2024	EACH OCCURRENCE \$1,000,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$300,000 MED EXP (Any one person) \$15,000 PERSONAL & ADV INJURY \$1,000,000 GENERAL AGGREGATE \$2,000,000 PRODUCTS - COMP/OP AGG \$2,000,000 \$
B	<b>AUTOMOBILE LIABILITY</b> <input type="checkbox"/> ANY AUTO <input type="checkbox"/> OWNED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS <input checked="" type="checkbox"/> HIRED AUTOS ONLY <input checked="" type="checkbox"/> NON-OWNED AUTOS ONLY			6081459486	8/15/2023	8/15/2024	COMBINED SINGLE LIMIT (Ea accident) \$1,000,000 BODILY INJURY (Per person) \$ BODILY INJURY (Per accident) \$ PROPERTY DAMAGE (Per accident) \$ \$
A	<input checked="" type="checkbox"/> UMBRELLA LIAB <input checked="" type="checkbox"/> OCCUR <input type="checkbox"/> EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE <input type="checkbox"/> DED <input checked="" type="checkbox"/> RETENTION \$10,000			6081459536	8/15/2023	8/15/2024	EACH OCCURRENCE \$15,000,000 AGGREGATE \$15,000,000 \$
A B	<b>WORKERS COMPENSATION AND EMPLOYERS' LIABILITY</b> ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	Y/N N	N/A	6081459522 (AOS) 6081459519 (CA)	8/15/2023 8/15/2023	8/15/2024 8/15/2024	<input checked="" type="checkbox"/> PER STATUTE <input type="checkbox"/> OTH-ER E.L. EACH ACCIDENT \$1,000,000 E.L. DISEASE - EA EMPLOYEE \$1,000,000 E.L. DISEASE - POLICY LIMIT \$1,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

**CERTIFICATE HOLDER**

\*\*For Information Only\*\*

**CANCELLATION**

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

KJ Wagner

© 1988-2015 ACORD CORPORATION. All rights reserved.

ACORD 25 (2016/03)

The ACORD name and logo are registered marks of ACORD



**ADDITIONAL REMARKS SCHEDULE**

AGENCY Edgewood Partners Insurance Center		NAMED INSURED Weaver and Tidwell, L.L.P 2821 W. 7th Street, Ste. 700 Fort Worth TX 76107	
POLICY NUMBER		EFFECTIVE DATE:	
CARRIER	NAIC CODE		

**ADDITIONAL REMARKS**

**THIS ADDITIONAL REMARKS FORM IS A SCHEDULE TO ACORD FORM,**

**FORM NUMBER:** 25      **FORM TITLE:** Certificate of Liability (03/16)

**HOLDER:** \*\*For Information Only\*\*

**ADDRESS:**

The General Liability and Automobile Liability policies include automatic additional insured endorsements providing primary/non-contributory coverage to any entity as required by written contract. All policies include blanket waiver of subrogation in favor of all entities required by written contract. 30 day notice of cancellation except 10 days for non-payment of premium included on the General, Auto, and Workers' Comp Liability policies. Excess Liability is "Following Form" and includes General , Auto and Employers Liability.