

**Notice of Meeting for the  
General Government and Finance Advisory Board  
of the City of Georgetown  
October 28, 2020 at 4:30 PM  
at Georgetown Public Library, 402 W 8th Street Georgetown, TX 78626**

The City of Georgetown is committed to compliance with the Americans with Disabilities Act (ADA). If you require assistance in participating at a public meeting due to a disability, as defined under the ADA, reasonable assistance, adaptations, or accommodations will be provided upon request. Please contact the City Secretary's Office, at least three (3) days prior to the scheduled meeting date, at (512) 930-3652 or City Hall at 808 Martin Luther King Jr. Street, Georgetown, TX 78626 for additional information; TTY users route through Relay Texas at 711.

**Consistent with Governor Greg Abbott's suspension of various provisions of the Open Meetings Act, effective August 1, 2020 and until further notice, to reduce the chance of COVID-19 transmission, all City of Georgetown Advisory Board meetings will be held virtually. Public comment will be allowed via teleconference; no one will be allowed to appear in person.**

**To participate, please copy and paste the following weblink into your browser:**

**Weblink:**

**Join Zoom Meeting**

**[https://georgetowntx.zoom.us/j/96359697305?](https://georgetowntx.zoom.us/j/96359697305?pwd=a3hHd2hhTWwvaWswSmdpTVJDZEx0Zz09)**

**[pwd=a3hHd2hhTWwvaWswSmdpTVJDZEx0Zz09](https://georgetowntx.zoom.us/j/96359697305?pwd=a3hHd2hhTWwvaWswSmdpTVJDZEx0Zz09)**

**Meeting ID: 963 5969 7305**

**Passcode: 086481**

**Dial by your location**

**888 475 4499 US Toll-free**

**833 548 0276 US Toll-free**

**833 548 0282 US Toll-free**

**877 853 5257 US Toll-free**

**Meeting ID: 963 5969 7305**

**Passcode: 086481**

**Find your local number: <https://georgetowntx.zoom.us/j/96359697305?pwd=a3hHd2hhTWwvaWswSmdpTVJDZEx0Zz09>**

**Citizen comments are accepted in three different formats:**

- 1. Submit written comments to [danella.elliott@georgetown.org](mailto:danella.elliott@georgetown.org) by noon on the date of the meeting and the Recording Secretary will read your comments into the recording during the item that is being**

**discussed.**

- 2. Log onto the meeting at the link above and “raise your hand” during the item.**
- 3. Use your home/mobile phone to call the toll-free number**

**To join a Zoom meeting, click on the link provided and join as an attendee. You will be asked to enter your name and email address (this is so we can identify you when you are called upon). To speak on an item, click on the “Raise your Hand” option at the bottom of the Zoom meeting webpage once that item has opened. When you are called upon by the Recording Secretary, your device will be remotely un-muted by the Administrator and you may speak for three minutes. Please state your name clearly, and when your time is over, your device will be muted again.**

**Use of profanity, threatening language, slanderous remarks or threats of harm are not allowed and will result in you being immediately removed from the meeting.**

---

## **Regular Session**

(This Regular Session may, at any time, be recessed to convene an Executive Session for any purpose authorized by the Open Meetings Act, Texas Government Code 551.)

- A Discussion on how this virtual conference will be conducted, to include options for public comments and how the public may address the Commission –Tommy Gonzalez, GGAF Chair
- B Review minutes from the August 26, 2020 General Government and Finance Advisory Board Meeting - Danella Elliott, Board Liaison
- C Presentation, discussion and update on mitigation since the 2018 risk assessment. – Mayra Cantu, Management Analyst
- D Consideration and possible action to recommend a resolution formally adopting the City’s Investment Policies for Fiscal Year 2021 – Leigh Wallace, Finance Director
- E Consideration and possible recommendation to Council of a contract with Suddenlink to provide dedicated Internet service for a total of \$136,620 over three years. - James Davis, IT Manager - Operations
- F Consideration and possible action to recommend to Council the purchase of vehicles and equipment in the amount of \$2,317,620 - Stan Hohman, Fleet Services Manager

## **Adjournment**

### **Certificate of Posting**

I, Robyn Densmore, City Secretary for the City of Georgetown, Texas, do hereby certify that this Notice of Meeting was posted at City Hall, 808 Martin Luther King Jr. Street, Georgetown, TX 78626, a place readily accessible to the general public as required by law, on the \_\_\_\_\_ day of \_\_\_\_\_, 2020, at

\_\_\_\_\_, and remained so posted for at least 72 continuous hours preceding the scheduled time of said meeting.

---

Robyn Densmore, City Secretary

City of Georgetown, Texas  
Government and Finance Advisory Board  
October 28, 2020

**SUBJECT:**

Review minutes from the August 26, 2020 General Government and Finance Advisory Board Meeting -  
Danella Elliott, Board Liaison

**ITEM SUMMARY:**

**FINANCIAL IMPACT:**

.

**SUBMITTED BY:**

Danella Elliott

**ATTACHMENTS:**

Description		Type
	08.26.2020 Draft Minutes	Backup Material

**Minutes of Meeting of the  
GENERAL GOVERNMENT AND FINANCE ADVISORY BOARD (GGAF)  
City of Georgetown, Texas  
August 26, 2020**

The General Government and Finance Advisory Board met on Wednesday, August 26, 2020 at 4:30 PM via Zoom virtual meeting.

The City of Georgetown is committed to compliance with the Americans with Disabilities Act (ADA). If you require assistance in participating at a public meeting due to a disability, as defined under the ADA, reasonable assistance, adaptations, or accommodations will be provided upon request. Please contact the City Secretary's Office, at least three (3) days prior to the scheduled meeting date, at (512) 930-3652 or City Hall at 808 Martin Luther King Jr Street for additional information; TTY users route through Relay Texas at 711.

The meeting was held with the Governor's Order, all City Buildings are following these procedures:

- Masks are recommended
- Physical distancing; 6 feet between you and anyone not in your household
- Practice good hygiene and wash your hands

**Board Members Present:**

Tommy Gonzalez, Chair  
Kevin Pitts, Vice-Chair  
Stu McLennan, Secretary  
Robert Witt

**Board Members Absent:**

Eric Corp

**City Staff Present:**

David Morgan, City Manager  
Laurie Brewer, Assistant City Manager  
Leigh Wallace, Finance Director  
Tadd Phillips, HR Director  
Laura Maloy, Assistant HR Director  
Holly Moyer, Benefits Consultant  
Greg Berglund, Assistant IT Director  
Eric Johnson, Facilities Director  
Trish Long, Facilities Superintendent  
Mayra Cantu, Management Analyst  
Danella Elliott, Board Liaison

**Others present:**

Rebecca Hawes, Gallagher Consultant

**Legislative Regular Agenda**

Tommy Gonzalez called the meeting to order at 4:41 p.m.

**A. Discussion on how this virtual conference will be conducted to include options for public comments and how the public may address the Commission – Tommy Gonzalez, GGAF Chair**

Tommy and Danella explained how the virtual conference would be conducted, including options for public comment.

**B. Review minutes from the June 24, 2020 General Government and Finance Advisory Board Meeting -Danella Elliott, Board Liaison**

Motion to approve the minutes by Stu McLennan; second by Kevin Pitts. Approved 4-0. Eric Corp absent.

**C. Consideration and possible action to award contracts for self-funded dental; program administration services, employee voluntary short-term and long-term disability insurance, employee supplemental insurance, an employee benefits concierge services authorizing the City**

**Manager to enter into such contracts on behalf of the City – Tadd Phillips, Human Resources and Organizational Development Director**

Tadd gave an overview presentation and noted that in response to the City’s competitively advertised RFP, a total of 21 proposals for one or more coverages were received Employee Health Benefit (including dental, voluntary short-term disability, long-term disability, supplemental insurance and benefits concierge services) for the upcoming 2021 calendar coverage year. He went over the process and timeline, as well as the scoring criteria.

Proposals were evaluated extensively by Human Resources, Gallagher and Co. (the City’s benefits consultant), and the Employee Benefits Committee, focusing on coverage offered as well as the financial impact. Finalists for major coverages were invited to make a presentation, and the City entered negotiations with the final candidates. Where possible, coverages were bundled during negotiations to achieve the best value for the City. RFP recommendations are for a proposed new vendor for dental and supplemental insurance, and maintaining the current vendor for disability and concierge services.

Based on the overall offering, financial impact on the City and the impact on employees, staff recommends GGAF approval to forward the following recommendations to Council:

<b>Program</b>	<b>Current Partner</b>	<b>Recommended Partner</b>
<b>Self-Funded Dental Administration</b>	Ameritas	<b>Guardian Life</b>
<b>Employee Supplemental Insurance</b>	Aflac	<b>Blue Cross Blue Shield TX</b>
<b>Employee voluntary short-term &amp; long-term disability</b>	Blue Cross Blue Shield TX	<b>Blue Cross Blue Shield TX</b>
<b>Benefits Concierge Services</b>	Alight (Compass)	<b>Alight (Compass)</b>

The City anticipates offering competitive benefits to employees while minimalizing the financial impact to both employees and the City. Contract and rate guarantee terms vary between one and year years, depending on program. Coverages will be reviewed during the year to evaluate performance, and the City has the option to renew for an additional year, saving the cost of processing an RFP, providing continuity in care to employees and allowing the City to establish an ongoing relationship with the provider.

The RFP included a mix of benefits paid by the employee, employer, and a combination of both. The four programs current annual cost to the City is \$168,076. The selected bids will result in an increase of \$1,596 or less than 1% increase. This is all within self-insurance fund budget.

Motion to approve Item C by Kevin Pitts; second by Stu McLennan. Approved 4-0. Eric Corp absent.

**D. Consideration and possible recommendation to approve a contract amendment and extension with Microsoft to provide Microsoft-branded software, and services to the City of Georgetown for a total of \$1,129,246.73 over 38 months. -- Greg Berglund, Assistant Director, Information Technology**

Greg Berglund, Assistant IT Director, explained that the City entered a three-year Enterprise Agreement with Microsoft in 2017. This agreement provides the City with licensing rights to install Microsoft products on City computer equipment, enables the IT Department to plan for enterprise upgrades to Microsoft software, utilizes Microsoft cloud services and provides software assurance which includes 24 x 7 technical support, access to the most current version of all applications, planning services, and technical training. Microsoft operating systems and software power every desktop, laptop and server on our computer networks. These tools enhance communication and collaboration and scale seamlessly with

growth while providing the top enterprise grade collaboration tools. These services have a financially backed 99.9% uptime service level and allow staff access to the tools across any internet connection. The City of Georgetown benefits heavily from having an Enterprise Agreement with Microsoft, and is a very cost-effective way to purchase these products.

The differences are: in 2017, we had 550 users, and in 2020 we are up to 900 users. We renegotiated the number of users and get more out of the licenses as well. Also included is enhanced security, included enabling two-factor authentication. The contract is more, but the actual per user license has decreased. The cost in 2017 was \$467 per user/per year, and the new contract is lower at \$396 per user/per year.

Staff recommends that the City approve a contract amendment and extension (for additional 38 months) of the City's Microsoft Enterprise Agreement.

Motion to approve Item D by Stu McLennan; second by Kevin Pitts. Approved 4-0. Eric Corp absent.

**E. Consideration and possible recommendation of approval to purchase laptops, desktops, and docking stations from Dell Inc. for an amount not to exceed \$199,971.08 -- Greg Berglund, Assistant Director, Information Technology**

Dell Inc. has been the City's vendor for desktop computers for approximately 10 years. In the first and second quarter of Fiscal Year 2020, the IT Department evaluated three vendors (Dell, HP, Lenovo) and determined Dell products to be the best value.

Implementation of these strategies over the next five years will prepare the City need to efficiently manage a hybrid environment that includes physical desktops and Cloud based virtual desktops.

Vendors were evaluated on:

1. Cost
2. Local economic impact of company
3. Responsiveness
4. Professional services
5. Product support offerings (City staff knowledge of the products (product options and fit with the City's internal support model)

In 2019, after conducting the study and a laptop computer pilot program, the City implemented a new strategy for the provision of desktop computers to employees to meet modern business needs and address technology changes. A five-year, three-pronged strategy was proposed to address these issues.

On March 24<sup>th</sup>, due to COVID-19, an item went straight to Council for approval to purchase 163 laptops and accessories for \$233,000. Employees needed to be able to have the equipment/technology quickly to be able to work remotely. This emergency purchase was approved, and that portion of the computer replacement project is completed. This has been reevaluated, and we would like to purchase the remaining equipment that was initially proposed in the 2020 budget as part of the City's desktop computer strategy implementation. Half of the planned purchase order was expedited in response to COVID-19 (mentioned above) and this request is to complete the original planned purchase.

Notes from Stu McLennan:

- Cost is \$199,971.08. Leverage DIR-TSO-3763 contract.
- OptiPlex 5070 desktops (x18)
- Laptops (x135); Dell Latitude 5420 (x20), Dell Latitude 5410 (x95), Mobile Precision 3551 (x20).
- Q1: Item Summary says laptops (x153). Typo?
  - A1. Yes.

- Confirm “and accessories”. Docking stations (x135); Dell Dock WD19 (x115) and Dell Thunderbolt (20)
- Planned for 2020. Expedited purchase of 50% due to COVID-19. This completes the buy.
- Q2: Did Council approve \$233,447 purchase @ meeting on March 24<sup>th</sup>?
  - A2. Yes.
- In 2019, CoG changed from its virtual desktop strategy. VDI underperformed and was labor intensive.
- CoG strategy now to purchase desktops (FY 20-22) and plan for cloud-based VDI (FY 22-24).
- GGAF discussed VMWare and cloud on May 29, 2019. Purchased 7x servers and VMWare software for primary datacenter. Dell agreed to buy replaced Cisco servers. Chris can see CoG moving to a cloud based capability in 5-years.

Staff recommends the purchase of 135 laptops, 18 desktops, and accessories.

Motion to approve Item E by Stu McLennan; second by Kevin Pitts. Approved 4-0. Eric Corp absent.

**F. Consideration and possible action to approve a Construction Contract with Brandt Companies, LLC, of Carrollton, Texas for the Construction of the Natatorium Pool HVAC Unit Replacement, at the Georgetown Recreation Center in the amount of \$607,077. – Eric Johnson, Facilities Director**

Eric went over the timeline for discussions on this topic, and explained that the original HVAC unit in the pool area of the Georgetown Recreation Center was in need of extensive repairs. The boiler is not in operation (it has no heat), one of the two circuits is down, the copper inside of the unit has extensive corrosion and is beginning to leak, and we performed repairs in 2019 totaling \$68K. The City contracted with Jose I. Guerra, Inc. (JIG) in 2019 to design a replacement unit for the pool area. They provided Construction Specifications and Construction Documents in June of 2020.

Trish Long provided the HVAC equipment inventory and noted that we have 449 pieces of equipment, and of that total, 49 contain R22. She explained that we will continue to budget replacement funds until R22 phase-out is complete. Approximately \$400K is budgeted in FY21.

On July 20, 2020, the City of Georgetown issued an Invitation to Bid for the Rec Center Natatorium Pool Unit replacement. On August 14, 2020 we received three (3) competitive bids. The low qualified bidder for the project was Brandt Companies, LLC with a total bid of \$607,077. Jose I. Guerra, Inc (JIG) has reviewed the submitted bid by the Brandt Companies. As a result of the findings JIG recommend the contract be awarded to Brandt Companies, LLC.

Notes from Stu McLennan:

- GGAF discussed on Feb 26, 2020. Estimated cost was \$700-\$800,000.
  - CoG budgeted \$800,000 in FY2020.
  - Funded by COOs in spring 2021.
- Action item submitted to Council on March 24<sup>th</sup>, June 9<sup>th</sup>, and June 23<sup>rd</sup>.
  - Council approved reimbursement resolution on June 23<sup>rd</sup>.
- \$68,000 in repairs in 2019.
- CoG issued RFP on July 20<sup>th</sup>. Received three proposals on August 14<sup>th</sup>.
- Q1: Why was DKC proposal \$910,000?
- A1: DKC is a GC. Markup is for overhead and profit. Other two are HVHC contractors.
- Trish Long, Facilities Superintendent.
  - CoG has 449x pieces of HVAC equipment.
  - 22x still have R-22.



Tommy reminded Eric that we needed to give the public as much notice as possible when the pool will be closing, and the expected duration of the closure.

Motion to approve Item F by Kevin Pitts, second by Stu McLennan. Approved 4-0. Eric Corp absent.

**G. Discussion and possible action to recommend Council adopt changes to the Fiscal and Budgetary Policy during the annual budget adoption process for Fiscal Year 2021 – Leigh Wallace, Finance Director**

Leigh presented the proposed changes to the Fiscal and Budgetary Policy for the upcoming budget.

The purpose of the Fiscal and Budgetary Policy is to provide the framework for financial operations of the City and to ensure prudent stewardship, financial planning and accountability. The bond rating agencies and external auditors are the primary external parties that review the policies and compliance. Leigh said that the goals was to find a balance between flexible enough to allow for situations that you may not can foresee until they happen, but also firm enough that they are guiding the organization in the right direction.

Each year the Policy is administratively amended to recognize date and amount changes within the text; and to address any new financial or regulatory requirement that may need to be added. Other amendments may be recommended to clarify wording or to further define a particular policy area.

Leigh gave some examples of past updates and explained the different types of changes usually included in the policy:

Potential administrative changes for consideration and discussion include:

- Clarify existing wording and formatting
- Remove old language that no longer applies
- Update compliance for coming fiscal year

Potential substantive changes for consideration and discussion include:

- Changing the meaning of the policy
  - Calculation change
  - Definition change
  - Change in decision maker
- Adding new policies

Leigh said that the COVID-19 pandemic was an opportunity to look at the policies in a new light, under circumstances that were emergency in nature and unusual compared to what they have typically been used for in the past. She is recommending broadening the wording in the within the budget contingency plan section to accommodate a wider variety of circumstances in which the plan may need to be used but still leaving in tact the actions that are authorized for the City Manager and City Council to take.

Other recommended changes are an update to the compliance within our own Capital Maintenance and Replacement and a change to our Debt Management Policy and Procedure, slightly broadening the wording of the method of sale.

Below is a recap of the recommended changes. There will be a Workshop with Council on September 8<sup>th</sup> and adoption of the policies will be an item on the September 22, 2020 Council meeting.

**Section IX. Budget Contingency Plan**

- FY2020 use of Budget Contingency Plan for first time in several years, and under new emergency circumstances
- Broaden the wording in the plan to accommodate a wider variety of circumstances
- Leave intact the actions authorized by City Manager and the Council

**Section XI. Capital Maintenance and Replacement**

- Economic changes resulting in decreased revenues
- FY2021 budget uses various reserves to sustain services/projects
- Reviewed with Council during budget development Page 9 of 167

**Section XIV. Debt Management**

- Collapse of the municipal debt market in March and April 2020 led City to postpone annual debt sale for capital projects
- Financial Advisor recommended various options
- Broaden wording for method of sale to include options other than competitive bidding
- Keep wording alternatives must be approved by Council

Section XV. Financial Conditions and Reserves

- Add GTEC and GEDCO reserves consistent with bylaws and existing practice
- Remove Downtown TIRZ debt service reserve no longer needed since Garage debt repurposed to Waste Transfer Station
- Add Cemetery reserve consistent with existing practice
- Georgetown Utility Systems Board re-organized to two separate boards to specialize in Electric Utility and Water Utility affairs
- Each board will review rates, contracts, and capital infrastructure plans
- Several additions/clarifications to the policies for FY2021 reflecting current practices
  - Opportunity to see policies in new light of pandemic circumstances
  - Use of reserves as planned during difficult economic environment and uncertainty
- City continues to be recognized by credit rating agencies for strong fiscal policies that emphasize flexible liquidity

Leigh will also add a reference to the Social Service Funding Policy when this presentation goes to Council.

Leigh explained that we do have 75 days of operating expenses (Citywide) and we do meet that reserve requirement. She feels confident/comfortable that we are using reserves in an appropriate way with language on how the reserves should be restored in the future and she feels very comfortable with that. She also mentioned that we have been recognized in the past by our credit rating agencies for our strong fiscal policies that recognize our flexible liquidity.

Discussion on some wording changes between Leigh and members, and she will make sure they are included in the correct locations throughout the policies.

Tommy suggested that Leigh send to all board members a listing of all reserves and what those dollar amounts are for each. Leigh said that it was in the budget document under the All Funds schedule, and totals about \$78M in all reserves for all 40ish funds across the city.

Notes from Stu McLennan:

- Proposed changes for 2021.
- Normally to GGAF and then Council in June-July. COVID-19 has affected that timeline.
- Section IX; Budget Contingency Plan.
  - Impact of pandemic.
- Split GUS Board.
  - Electric Utility - Electric.
  - Water Utility - Water and Wastewater.
- Section XV; Financial Conditions and Reserves.
  - Add GTEC and GEDCO reserves.
  - Remove Downtown TIRZ debt service reserve. No longer needed.
  - Add Cemetery reserve.
- Leigh explained IT recovery rates vis-à-vis the purchase of fiber assets from the Electric Utility Fund. Section XI(C)(2). Annually in 2021 to 2023, CoG will save 20% over IT's 90-day Capital Reserve Fund Balance to facilitate this purchase.
- CoG currently has \$78 million in 90-day reserves for 40 funds.
- Since 2012, the CoG has used \$5 per capita based on 71,000 residents. Currently overfunded since CoG is ~60,000 residents. US Census reflects 79,000.

Motion to approve Item G (with the recommended changes) by Kevin Pitts, second by Stu McLennan. Approved 4-0. Eric Corp absent.

Motion to adjourn meeting by Stu McLennan, second by Kevin Pitts, approved 4-0. Meeting adjourned at 5:55 pm.

---

Tommy Gonzalez  
Board Chair

---

Date

---

Stu McLennan  
Board Secretary

---

Date

---

Danella Elliott  
Board Liaison

---

Date

City of Georgetown, Texas  
Government and Finance Advisory Board  
October 28, 2020

**SUBJECT:**

Presentation, discussion and update on mitigation since the 2018 risk assessment. – Mayra Cantu, Management Analyst

**ITEM SUMMARY:**

In 2018 the city had an enterprise risk assessment conducted by Plante Moran. The risk assessment detailed several risks across the various departments and highlighted mitigation we were doing at the time, recommendations on how to address some rising risks, and staff's response to the recommendations. Since then several mitigation efforts have occurred in response to the risk assessment. This presentation provides an update and overview of the mitigation efforts that are ongoing, completed, and some near-term actions staff will complete to further mitigate risk across the City.

**FINANCIAL IMPACT:**

.

**SUBMITTED BY:**

Sharon A Parker

**ATTACHMENTS:**

	<b>Description</b>	<b>Type</b>
□	RMR	Presentation
□	Risk Mitigation Report	Backup Material
□	Georgetown Risk Assessment	Backup Material

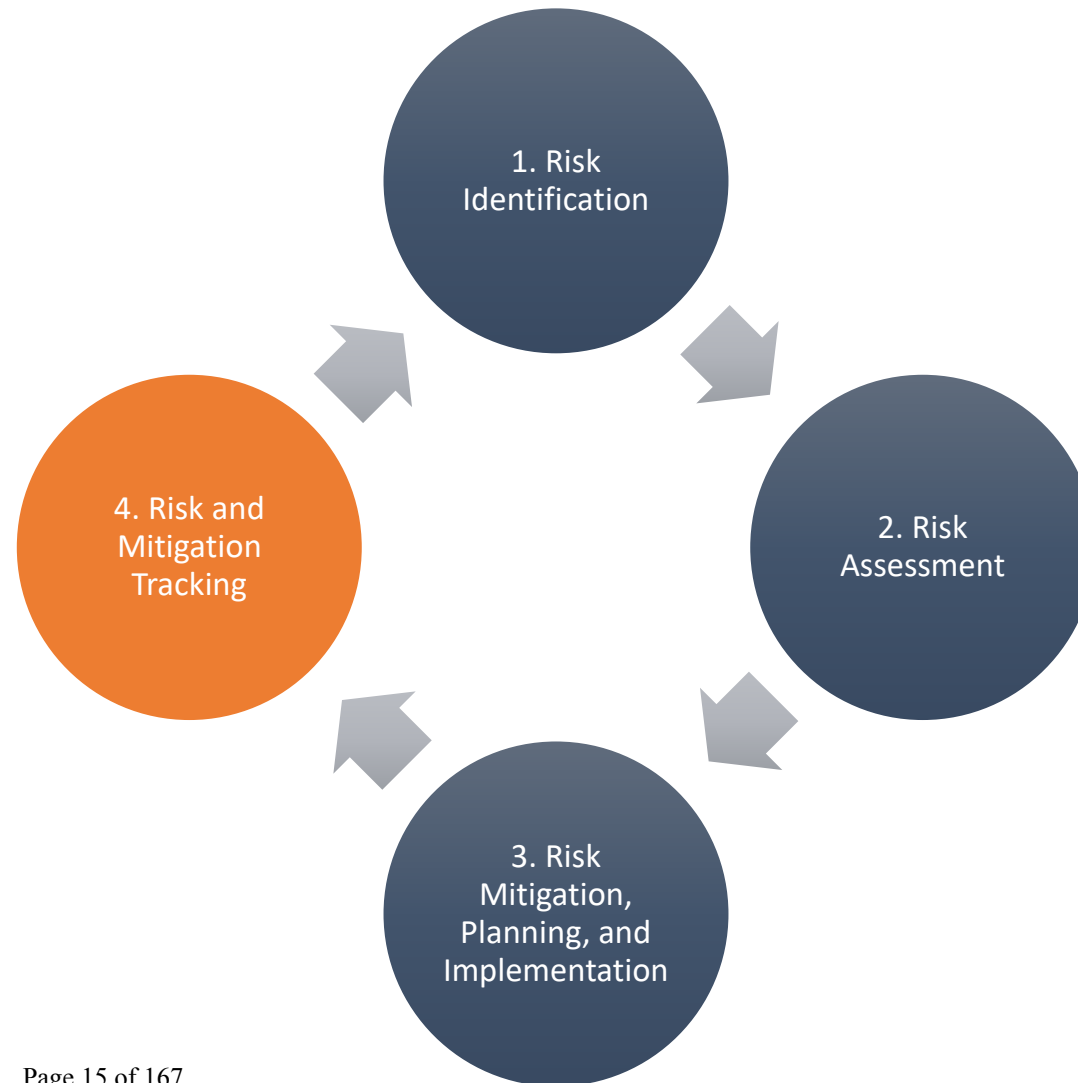
# Risk Mitigation Report

---

# OVERVIEW

- Introduction
- 2018 Risk Assessment
- Mitigation Completed
- Recommendations

# RISK CYCLE



# DEPARTMENTS/DIVISIONS

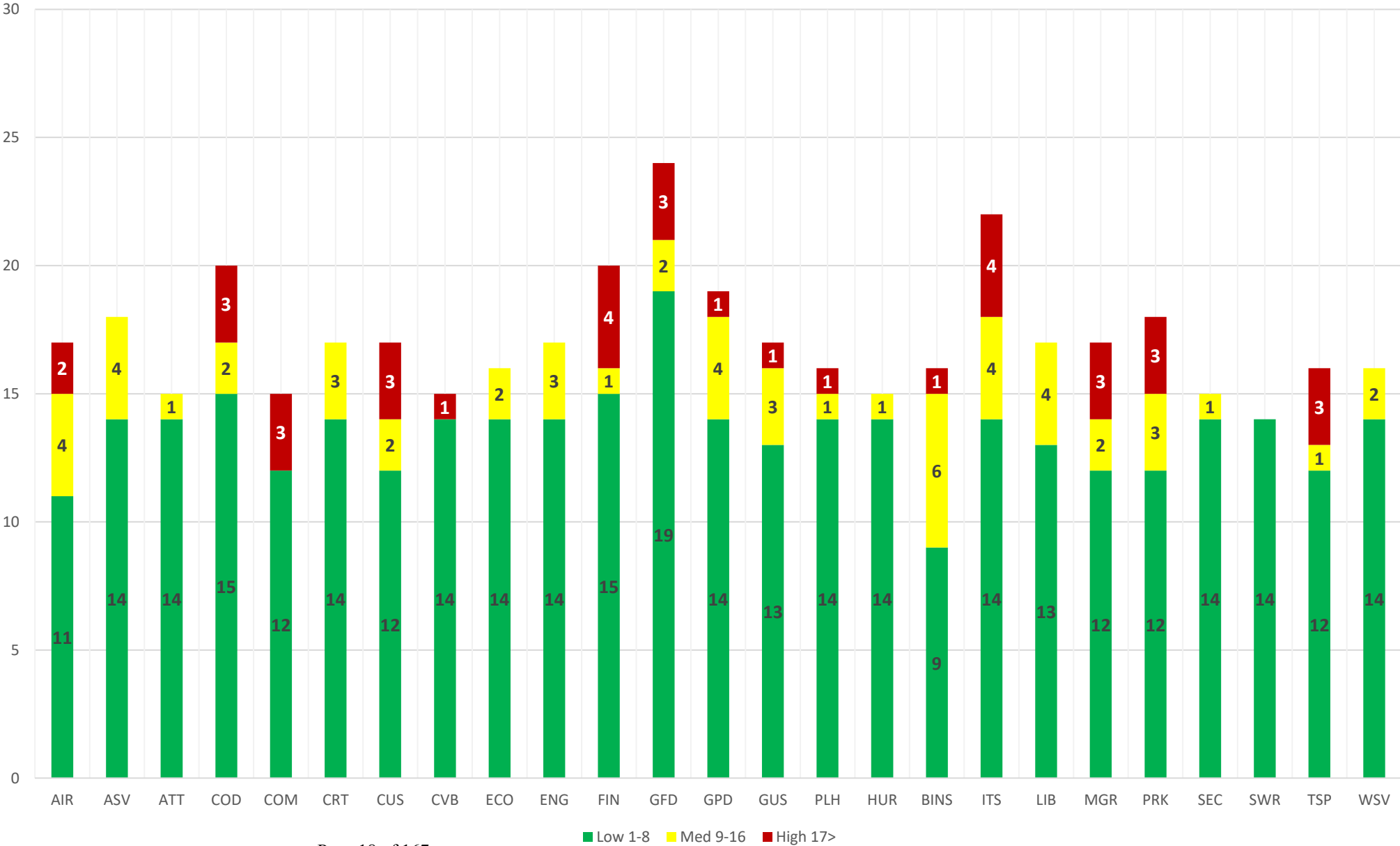
- City Secretary
- City Manager's Office
- Controller
- Emergency Management
- Facilities
- Finance
- Fire
- Human Resources
- Information Technology
- Parks
- Police
- Purchasing
- Records
- Utility (Customer Care, Water and Electric)



# RISK UNIVERSE

City of Georgetown Risk Universe	
Access to Talent	IT Security Awareness, Training, and Education
Billing for Citizen Services	IT Third Party Roles and Responsibilities
Budget and Planning	Leadership
Composition of Tax Base	Legislation
Disaster Recovery/Business Continuity	Physical Security
Emergency Notification System Failure	Police failure
Fire Department Failure	Records Management
Freedom of Information Act (FOIA)	Regulatory Filings
Fraud	Segregation of Duties
Grant Obligations	State-Fed Regulations
Health & Safety	Succession Planning
IT Access Management	Talent Management
IT Asset Management: Data Classification	Tax
IT contingency Plan	Utility market
IT Critical Security Event Identification	Utility Outage
IT Cybersecurity Governance Model	Vendor Reliance
IT Incident Response Management	

2018 Residual Risks by KBD



# MITIGATION SUMMARY

IMPACT / OCCURRENCE LIKELIHOOD LEVEL	2018 Risks	Fully Mitigated	Partially Mitigated	Not Mitigated
HIGH	5	2	3	0
MEDIUM	17	5	12	0
LOW	11	6	4	1
Total	33	39%	58%	3%

# SIGNIFICANT CHANGES SINCE 2018

- **Electric Utility-Energy Portfolio Management**
- **Reorganization of City**
- **Workday ERP**
- **COVID-19**
  - Impact On FY2020 Budget And Beyond
- **Lost EMS iPad**
  - Possible HIPAA Breach
- **Senate Bill 2 (revenue caps)**
- **Shot Clock Legislation**
- **Back-Up Data Center**

# MITIGATION-INFORMATION TECHNOLOGY

## Cybersecurity Policy

- Completed a primary draft of a comprehensive Cybersecurity Policy, currently under review by the legal department.

## System and Network Contingency Plan

- Incident Response Plan in development. This plan is scheduled for completion in December of 2020.

## Security Information and Event Management System

- Multiple Security Information and Event Management Systems (SIEMs) are under review by the IT Department.
- IT Department is evaluating the possibility of managed service contracts through the Texas Department of Information Resources to help fulfill this need.

# MITIGATION-INFORMATION TECHNOLOGY

## Staff IT Security and Awareness Training

- Successfully implemented a Security and Awareness Training initiative in FY 2020.
- In June of 2020, the City Security Awareness Training program was certified by the State of Texas as complete for the current calendar year.

## Secondary Back-Up Data Center

- A back-up data center was successfully brought online in the Winter of FY 2020. The purpose of this data center is to act as a failover in the case of a failure at the City's primary data center.

## Homeland Security Audit

# MITIGATION-PUBLIC SAFETY

## HIPAA Audit

- The audit identified measures that need to be taken to maximize the protection of private health information and has informed a work plan for staff to reduce the risk of a breach occurring.

## Guardian Tracking – Police Performance Management Software

- The software is used to formally capture praise, counseling, goal setting, and discipline.
- The software also serves as an early warning system for repeated substandard performance.

## CommUNITY Advisory Task Force

- Established in July of 2020 comprised of 20+ diverse community leaders. The task force will be working with the Chief to provide input regarding the state of policing in Georgetown as well as providing input as to the direction of the CommUNITY Initiative.
- The police department plans to conduct six Listen and Learn Summits across six different stakeholder groups in FY2021.

# MITIGATION-PUBLIC SAFETY

## Police Training – Arbinger Institute

- The police department is in the process of having their officers complete training created by the Arbinger Institute. This training focuses on transitioning a self-focused inward mindset to an impact-focused outward mindset
- Focuses on situational awareness and officer safety, trust and collaboration, and leadership.

## *Replacement of Police Body Cameras*

- All cameras and the digital data derived are on one unified management software system.
- The current technology is far superior to the old allowing for real time viewing, wider angles, seamless integration between car and body cameras, and automatic synchronization of all incident cameras on playback.

## Fire Station 6 and 7

- Fire Station 6 is open and 7 is set to open soon, adding additional resources to key areas within the City for a more efficient response. Fire station 7 will also add an engine and ambulance to our EMS system.



# MITIGATION – EMERGENCY MANAGEMENT

## COVID-19 Response

- The City is working closely with Williamson County, the Williamson County and Cities Health District, and State partners to coordinate our response to the pandemic.
- The City has created an inventory of personal protective equipment to ensure adequate supplies both for first responders and general employees to be appropriately protected.
- The City has amended internal personnel policies to ensure appropriate social distancing at work, allowing employees to telework when appropriate, and appropriate measures are taken when employees test positive for COVID-19

## Hazard Mitigation Action Plan

- The plan helps the City appropriately assess, prioritize, prepare for, and mitigate natural or human-caused hazards. This plan will allow the City to maintain eligibility for future federal mitigation grant funding and help identify mitigation actions that will make the local community more disaster resistant

## Planning

- Select staff recently completed a tabletop exercise on a cybersecurity event. In tabletop exercises key personnel who have emergency management roles and responsibilities gather to discuss various simulated emergency situations. This allows the City to think more proactively and align possible response efforts to events that could happen.

# MITIGATION – CITY SECRETARY'S OFFICE

## Freedom of Information Act

- The Open Records Coordinator will continue to provide annual trainings to staff related to best practices for responding to FOIA requests and do routine reviews of the Open Records Request policies and procedures.

## Records Management

- The Records Management Team does a routine review of the Records Management policies and procedures to ensure that best practices are always being implemented.
- Provide annual training to all employees

# MITIGATION – FACILITIES

## Facility Access Policy

- City Facilities are migrating to a public lobby and secure back of house model,
- This policy will help establish necessary employee access to non-public areas within City Facilities.

## Georgetown Municipal Complex(GMC) Remodel

- Secure separation of public and employee space requires building modifications, including access control doors and publicly accessible meeting space to keep employees from bringing public into the secure space.

## HLWW Remodel

- Building currently requires entry from an alley and there is no separation from the public space and employee areas.
- Remodel moves the front Planning entry to Martin Luther King Jr. St.
  - Will allow the use of a public lobby with a secure door to the employee area.

# MITIGATION – CITY MANAGER’S OFFICE

## Organizational Performance Management

- The City Manager’s Office routinely reviews departments performance metrics. On a biannual basis the metrics are reviewed and analyzed for performance.
- Allows CMO to address area of concerns
- Further supports budget requests given data

## Business Plans

- The City had all departments and service areas create and complete business plans that help strategically align the departments missions and goals to objectives that will be completed over the next few years.
- Reviewed regularly by management to ensure action plans are being completed.

## Legislative Advocacy

- The Legislative Task Force is a special ad hoc group comprised of active leaders in the community - the leadership of City Boards and Commissions.
- The Legislative Program will provide input to City Council on the issues relevant to the State Legislative Agenda in preparation for the Texas State Legislative Sessions.
- Communicate to create stronger public engagement and advocacy with the legislature

# MITIGATION - FINANCE

## Financial and HR Management/Workday

- This new system has aligned financials and human resources to one system streamlining purchasing, travel, hiring, accounting, and budget to name a few high-level processes
- Conducted detailed process reviews to implement best practices
- Enhanced user and access controls
- Created process controls such as budget checks on purchases and created a system of multi-level of approvals for purchases
- Created better reporting
- Implementing a budget module and project module to streamline and integrate workflows within the Workday system

# MITIGATION - FINANCE

## Internal Audit Plan

- Staff is creating a multi-year internal audit to apply a disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.
- Some of the audits staff are including in the audit plan are:
  - Fee Collection Review
  - Hotel/Motel Audit
  - Franchise Fees
  - Airport Revenue

# MITIGATION - FINANCE

## Sales Tax Audit of City Enterprise Revenue

- The State is currently conducting a sales tax audit of revenue from city services that began in June 2020.
- The audit helps determine whether taxes have been properly collected from city services, reported, and paid to the state. (Electric, Garbage, Airport)

# MITIGATION – HUMAN RESOURCES

## Business Plans

- The City had all departments and service areas create and complete business plans that help strategically align the departments missions and goals to objectives that will be completed over the next few years.
- Reviewed regularly by management to ensure action plans are being completed.

## Organizational Development

- The City hired its first learning and development coordinator in 2020. The coordinator has built a learning and development strategic plan that will be deployed over the next two years.
  - Plan includes multiyear approach to talent management and making use of Workday talent capabilities
- In 2019 the City created the organizational & operational excellence office
  - The office has since rolled out annual business plans for all departments, lean trainings, and currently support over 60 lean process improvement projects.



# MITIGATION – HUMAN RESOURCES

## Policy Updates

- Six personnel policies were updated in alignment with Workday implementation in 2019 including introductory period, vacations, sick leave, hours of work, compensatory time, and holiday.
- Multiple temporary policies have been issued during the COVID-19 Pandemic including telework and flex time.

## Safety & Risk Management Team

- The City's safety and risk management programs were combined, centralized, and staffed by three full-time employees focused on the development and evaluation of occupational safety and risk management programs in 2019.
- Improved handling of citizen claims, accuracy in covered city property, management of our third-party risk pool administrators, and given greater support to our employees who experience work-related injuries
- Building data sets to better understand worker injury and accident trends and working with stakeholders on appropriate mitigating actions

# MITIGATION - UTILITIES OVERALL

## Weaver Assessment – Cash Receipt Review

- Assisted in the review and identification of all cash receipts currently received the by City's Utility Billing Office
- Provided risk-control matrices and process mapping for areas in the City's Utility and Accounting Offices where internal risks could occur.

## Weaver Assessment – UMAX Business Process Mapping

- Provided a review of the City's Utility Office internal controls, transactional processing efficiencies and review of audit trails and automated workflows integrated in the City's new UMAX/CIS.
- Documented workflows that are used when reviewing business processes.
- The high-risk areas have been mitigated and many of the moderate risks have been addressed.

# MITIGATION - UTILITIES OVERALL

## Gartner Assessment – AMI/CIS and MDM Systems

- Conduct an assessment an analysis of the City's Customer Information System (CIS), Advanced Metering Infrastructure (AMI) and Meter Data Management (MDM) systems.
- Evaluated the City's CIS business processes against the current CIS system, identify gaps or areas for opportunities, and explore alternative options to improve the City's CIS operations and supporting technologies

# MITIGATION - ELECTRIC

## Adoption of comprehensive Energy Risk Management Program

- Implemented an Energy Risk Management Policy which governs all purchase power and related activities that may impact the Energy Risk profile of Georgetown Electric Utility.
- Overall policy oversight is provided by City Council and the Georgetown Electric Board (GTEB). Independent 3rd Party provides Risk Management Compliance reporting to GTEB and City Council.

## Risk Oversight Committee

- The Risk Oversight Committee (ROC) is an internal committee that oversees approval and compliance of transactions and risk limits.
- The committee is comprised of the City's executive team (City Manager and Assistant City Managers), the Electric General Manager and staff, and the Finance Director.

## Risk Management Committee

- The Risk management Committee (RMC) is comprised of Shell, the Electric General Manager and staff, as well as independent consultants.
- The RMC implement the risk management strategy approved by the ROC. The RMC reviews existing and potential transactions, monitor proximity to limits, and helps support the responsibilities of the ROC.

# MITIGATION - ELECTRIC

## 3<sup>rd</sup> Party Electric Portfolio Management

- Shell will be developing and making recommendations regarding how Georgetown's energy is traded in the Texas energy market.
- Shell will also assist in forecasting energy needs, energy costs, and addressing challenges related to transmitting energy around the state, all of which affect the city's costs associated with purchasing power.
- In addition to Shell North America, Crescent Power and ACES Power Marketing aid the staff in managing the overall energy portfolio risk and risk management policy compliance.

## Electric Board

- Starting June 2020, a new electric oversight board was set up. Aid the City Council in providing the overall Policy Oversight.

# MITIGATION - ELECTRIC

## Line Extension and Meter Connect Revenue Risk Mitigation

- Review of the revenue generating activities related to electric infrastructure additions and service provisioning identified revenue loss and revenue leakage
- Mitigation activities:
  - Business re-organization led to the electric engineering and project management function under the electric cost center. This identified the revenue losses and the redesigned processes led to better control and management of the electric infrastructure additions with appropriate cost recovery.
  - New Electric line extension policy implemented in early part of FY 2020, clearly identifies the infrastructure addition costs and the requirement of pre-payment of the invoices mitigated the risks posed by unpaid/overdue invoices.
  - Short term mitigation strategies were identified which address the meter connect revenue loss. The long-term mitigation strategy of a comprehensive business process redesign of the utility service connection is in progress. The new process will be in place starting January 1<sup>st</sup>, 2021.

# MITIGATION - WATER

## Risk Assessment

- The water utility had a risk and resilience assessment conducted by CDM Smith to comply with a new mandate set by the American Water Infrastructure Act. The assessment outlined several recommendations to help mitigate risks and improve system resiliency against the highest risk threats identified.

## Succession Planning

- The Water Utilities Director is set to retire by the end of the year.
- The City has started a plan to begin a national search for the next water utility director. In the meantime the Director has informally begun to prepare his direct reports to be able to assume more responsibility and is training them on any knowledge gaps he foresees.

## Water Rate Study

- The city continues to maintain utility fiscal health by performing rate study and impact fee studies every three years. Previous rate studies were conducted on a revenue sufficiency principal. The rate study currently is a cost-of-service rate study.
- The water rates and tiers were evaluated primarily for residential customers and will be in effect 2021.

# MITIGATION - WATER

## Long Term Water Planning

- The BRA and the City of Georgetown are jointly funding and participating in an Aquifer Storage and Recovery (ASR) Study.
- The BRA, City of Round Rock and Georgetown are jointly participating in a collaborative study to identify regional and long-term water solutions for Williamson County.
- Working to include additional groundwater resources from counties to the east as a long-term water resource within the Region G Plan.

## Capital Improvement Projects

- Increasing treated water capacity
- Maintaining infrastructure at the rate of the City's growth



# MITIGATION - WATER

## System Interconnects

- The City is further diversifying its water resources and increasing system resilience through interconnects with neighboring systems.
- The City currently has two interconnects with Round Rock and a third under design to utilize Round Rock's excess treatment capacity.
- An additional short-term interconnect is also constructed between the City and Leander's system.

## Water Leak Detection

- Starting in Fiscal year 2021, the city will be improving leak detection by using satellite detection. The City's vast service area makes this method of detection and subsequent repair more efficient.

# NEAR TERM ACTIONS

- **Conduct a citywide operational and enterprise risk assessment every 5 years- with the next study slated for FY23**
- **Complete Hazard Mitigation Plan**
- **Implement consultants' recommendations as a result of the following studies:**
  - Gartner Assessment of CIS/AMI/MDM systems
  - HIPAA Audit by SHI
- **Conduct an audit of the electric risk management practices**

# NEAR TERM ACTIONS (Cont.)

- **Finalize and initiate internal/external audit work plan**
- **Process improvement:**
  - Streamline purchasing process and create training for power users to ensure compliance with procurement laws
  - Integrated Council agenda process across the City Manager's Office, City Secretary's Office, City Attorney's Office and Purchasing department as well as creating and implementing training for power users on the agenda process
- **Overall biannual review and update of citywide and departmental policies and procedures**
- **Providing public dashboards of departmental performance management metrics**

# QUESTIONS?



# Risk Mitigation Report

UPDATE TO 2018 CITYWIDE RISK ASSESSMENT



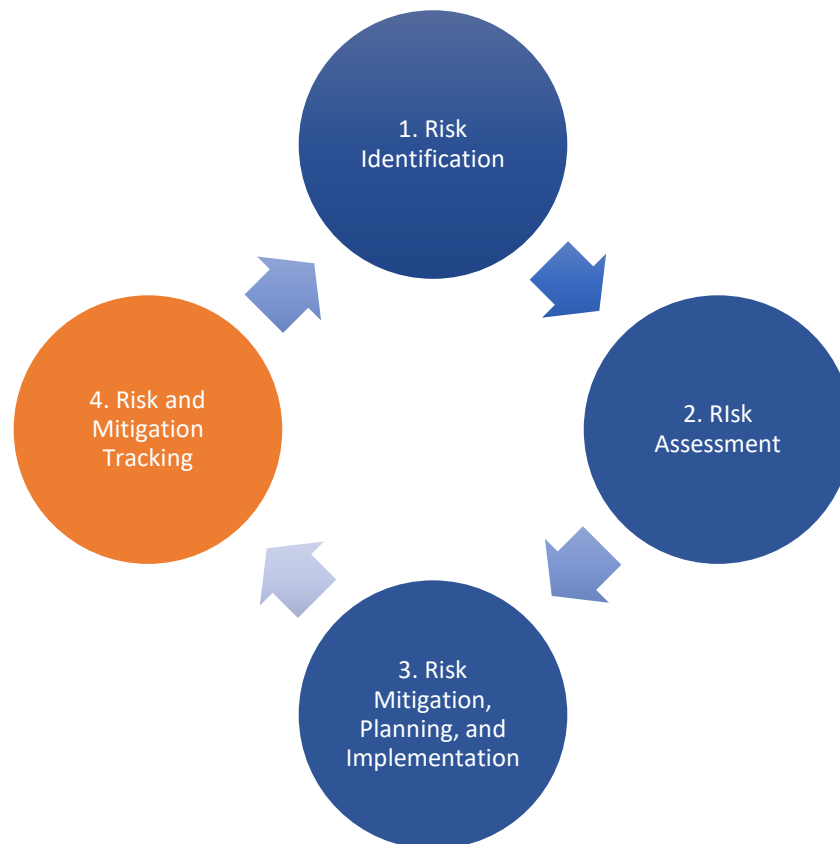
## Table of Contents

<b>Purpose and Introduction .....</b>	<b>2</b>
<b>Risk Assessment and Mitigation Cycle .....</b>	<b>2</b>
<b>Risk Management Methods.....</b>	<b>3</b>
<b>Notable Changes .....</b>	<b>4</b>
<b>Departments.....</b>	<b>4</b>
<b>2018 Citywide Risk Assessment.....</b>	<b>5</b>
<b>Mitigation and Next Steps .....</b>	<b>8</b>
City Manager’s Office.....	8
Facilities .....	8
Emergency Management.....	9
Public Safety.....	9
Finance and Human Resources.....	11
City Secretary .....	13
Information Technology.....	13
Overall Utility System.....	14
Electric.....	15
Water and Wastewater System .....	17
Public Works .....	19
<b>Near Term Action .....</b>	<b>20</b>
<b>APPENDIX.....</b>	<b>21</b>
Risk Mitigation Register .....	21

## Purpose and Introduction

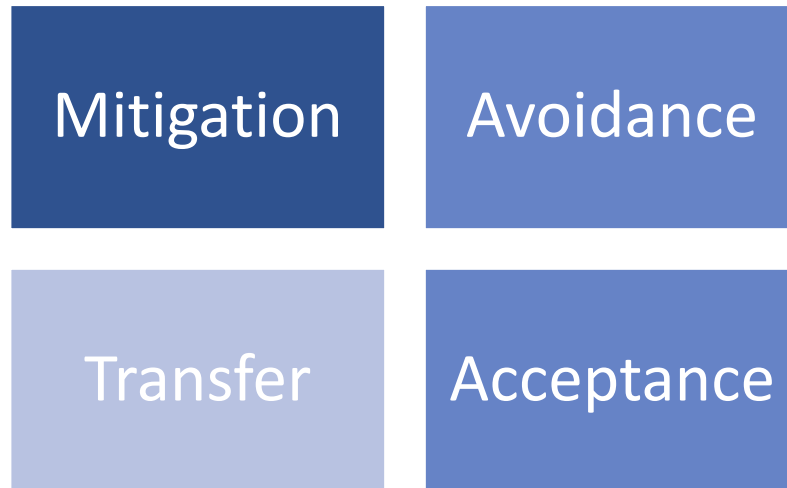
In 2018 a citywide risk assessment was conducted by Plante Moran, which outlined several risks across departments. Plante Moran also included risk treatment action plans for the risks they identified with recommendations on ways to mitigate in the future to reduce the risk likelihood or impact. This report outlines the mitigation and risk treatment statuses of the identified risks from 2018.

## Risk Assessment and Mitigation Cycle



Steps 1-3 of the risk cycle were completed at different stages since 2018. After the risk assessment was conducted, the City has been in the 3<sup>rd</sup> part of the cycle with risk owners treating their risk with varying degrees of mitigation. The City now concurrently enters the last step of the cycle, step 4, as each risk is reviewed, and mitigation efforts are tracked to reassess whether the risk score has decreased. After this is completed the City will need to have another citywide ERP risk assessment conducted by 2023 to successfully identify new risks across the city from an enterprise and operational standpoint.

Overall, most risks identified in 2018 have been mitigated or the risk has been accepted and steps are being taken to fully mitigate in the future as detailed later in this report.



### **Risk Management Methods**

Risk does not always have to be mitigated. Several risk management methods exist that can be used instead to either eliminate a risk with risk avoidance, transferred to a third party with risk transfer, or even accepted because the risk is negligible that it would cost more to manage it than what it could possibly impact.

#### **Risk Mitigation**

Risk mitigation is a risk management technique by which an organization introduces specific measures to minimize or eliminate unacceptable risks associated with its operations. Risk mitigation measures can be directed towards reducing the severity of risk consequences, reducing the probability of the risk materializing, or reducing the organizations exposure to the risk.

#### **Risk Avoidance**

Risk avoidance is a technique of risk management where the goal is to eliminate a risk and not just reduce it. Rather than mitigating existing risk, it aims to eliminate the source of the risk altogether, sometimes replacing it with a smaller, more easily manageable risk.

#### **Risk Transfer**

Risk transfer is a risk management technique in which risk is transferred to a third party. In other words, risk transfer involves a party assuming the liabilities of another party. Purchasing insurance is a common example of transferring risk from an individual or entity to an insurance company.

#### **Risk Acceptance**

Risk acceptance is the assumption of a risk, typically because its risk-reward profile is attractive and within your risk tolerance. In general, it is impossible to make gains in business or life without taking risks. As such, risk acceptance is a common risk treatment.



## Notable Changes

Significant events and operational changes since the 2018 citywide risk assessment update—include the following:

- 3<sup>rd</sup> party electric energy portfolio manager
- City department reorganization
- Workday ERP
- COVID-19; impact on FY2020 budget and beyond
- Police and Fire agree and confer
- Finance bond rating
- In the spring of 2019, the Fire Department filed a “breach notification” report regarding an unencrypted EMS tablet that went missing from one of the ambulances. This breach had the potential to impact up to 719 patients.

The 2018 Risk Assessment identified the most prevalent risks lived within the following departments.

## Departments

- |                           |                          |
|---------------------------|--------------------------|
| • City Secretary’s Office | • Information Technology |
| • City Manager’s Office   | • Facilities             |
| • Controller              | • Police                 |
| • Emergency Management    | • Purchasing             |
| • Finance                 | • Records                |
| • Fire                    | • Utility                |
| • Human Resources         |                          |

## 2018 Citywide Risk Assessment

The risk assessment conducted in 2018 established the following risk universe for the City of Georgetown.

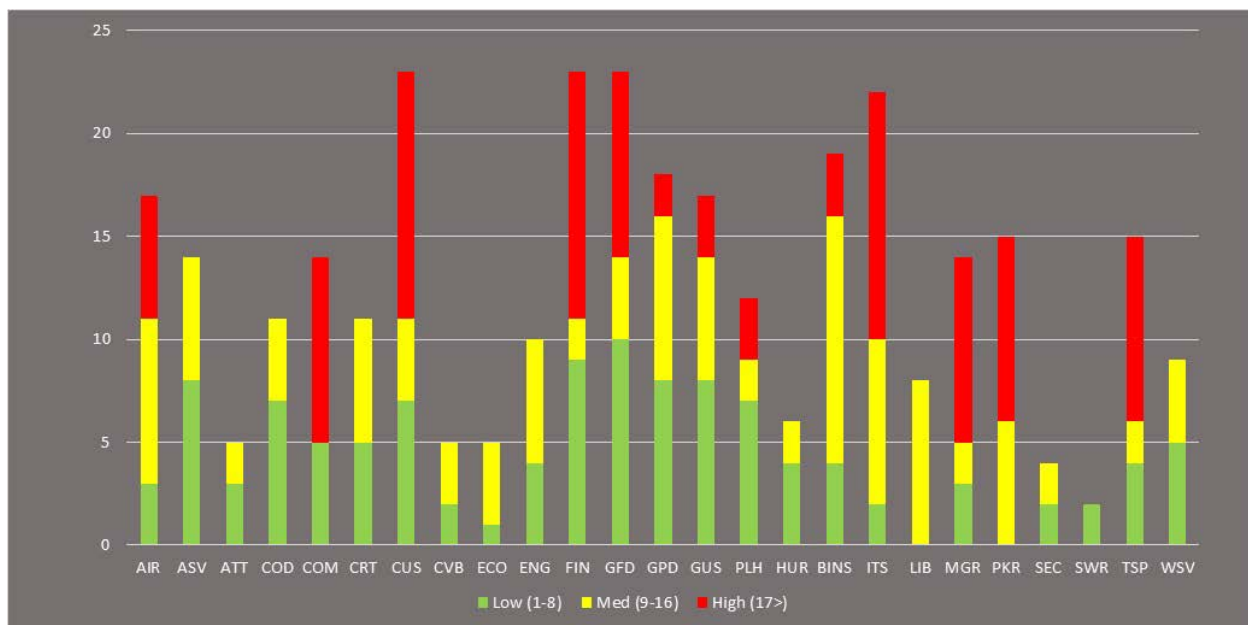
City of Georgetown Risk Universe	
1. Access to Talent	18. IT Security Awareness, Training, and Education
2. Billing for Citizen Services	19. IT Third Party Roles and Responsibilities
3. Budget and Planning	20. Leadership
4. Composition of Tax Base	21. Legislation
5. Disaster Recovery/Business Continuity	22. Physical Security
6. Emergency Notification System Failure	23. Police failure
7. Fire Department Failure	24. Records Management
8. Freedom of Information Act (FOIA)	25. Regulatory Filings
9. Fraud	26. Segregation of Duties
10. Grant Obligations	27. State-Fed Regulations
11. Health & Safety	28. Succession Planning
12. IT Access Management	29. Talent Management
13. IT Asset Management: Data Classification	30. Tax
14. IT contingency Plan	31. Utility market
15. IT Critical Security Event Identification	32. Utility Outage
16. IT Cybersecurity Governance Model	33. Vendor Reliance
17. IT Incident Response Management	

Each department has at least one of the above risks identified. Plante Moran worked with the departments to identify management responses to mitigate those risks at the time and outlined next steps to further mitigate the risks. The risks were given a risk impact score which was calculated utilizing ranked criteria: impact (financial, strategic, operational or compliance) and likelihood (probability or event occurrence) as noted below.

Impact Criteria					
Ranking	5 (high)	4	3	2	1 (low)
<b>Financial Impact:</b>					
Expense or Lost Revenue	>\$150K	\$100K-150K	\$50K-\$100K	\$25K-\$50K	<\$25K
<b>or Strategic Impact:</b>					
Strategy/Mission/Legislature	Failure to meet key strategic objective	Major impact on strategic objective	Moderate impact on strategy	Minor impact on strategy	No impact on strategy
<b>or Operational Impact:</b>					
Reputation	Extreme	Severe	Moderate	Low	None
Process/System Shutdown	>7 days	5-7 days	3-5 days	1-3 days	<1 day
<b>Compliance Impact:</b>					
Regulatory-State/Local/HIPAA/Debt Covenants	Large-scale material	Material breach but	Material breach which can	Minimal breach which	Minimal breach which can

	breach of regulation	cannot be rectified	be readily rectified	cannot be rectified	be readily rectified
<b>Likelihood Criteria</b>					
<b>Ranking</b>	<b>5 (high)</b>	<b>4</b>	<b>3</b>	<b>2</b>	<b>1 (low)</b>
<b>Probability of an event occurring in a given year:</b>					
	>20%	15-20%	10-15%	5-10%	<5%
<b>or Event Occurrence (on average):</b>					
	Once a year or more	1 in 3 years	1 in 5 years	1 in 7 years	1 in 10 years

## 2018 Residual Risks by KBD:



Weighted Risks by Key Business Departments: the total number of risks weighted by rankings using the following weighting formula: Red 17 or > (3 points), Yellow 8-16 (2 points), and Green <8 to 5 (1 point), <4 (0 points). Therefore, the higher risk rankings carry a higher weighted risk.

Since then these risks have been primarily mitigated, and a detail can be found in the appendix.

The 2018 risk assessment highlighted several high-level themes, particularly focused in Information Technology, Georgetown Utility Services, legislation, and policies and procedures. Since 2018, several strides have been made in each of these high-level themes.

### High-Level Themed Risks

- The City is exposed to four high Information Technology (IT) residual risks. We recognize the City is currently in process of an ERP system upgrade and the status of these conditions will change in the near future: IT Cybersecurity, IT Asset Management: Data Classification, IT Access Management, and IT Contingency Plan. See Appendix B for IT Risk Report.

- The City lacks a clear process for the assignment and review of user access roles and responsibilities to achieve segregation of duties in three key business departments. We noted during discussions with Finance, Customer Care and Parks and Recreation one person can control more than two phases of a transaction exposing the City to unauthorized transactions and fraud risk.

- Management indicated several potential costly Texas legislative acts are due for review at future legislative sessions.

- The City is challenged with documentation of operating policies and procedures. Currently, 15 out of 25 (60%) departments we interviewed have a lack of clearly written policies and procedures available to all employees

### Risk Treatment Responses and Mitigation

- IT is working on a comprehensive policy covering IT Cybersecurity, IT Asset Management: Data Classification, IT Access Management, and IT Contingency Plan.

- Workday has mitigated this risk, with various level of approvals needed for transactions. The requisitioner must have each requisition reviewed and approved by at least two people, with one being the manager. The risk of fraud has been mitigated significantly, if not almost entirely with the new ERP system and its integrated steps for accountability.

- Staff has created an Intergovernmental Affairs Program which will prioritize the City's legislative agenda considering public input; a committee is being created to enact this program. Focused Advocacy has also been hired as a consultant to aid in representing the City in legislative session. The City of Georgetown is also a participating TML city, allowing TML to provide guidance, direction, and advocacy on behalf of City's best interests.

- Since 2018 many of the lacking policies have now been written, with even more reviewed. Staff has identified a need to centralize a location for its policies and create a process or committee to review policies regularly to ensure they are up to date and follow legal mandates.

## **Mitigation and Next Steps**

The departments identified in the 2018 risk assessment have taken several mitigating steps which are fully detailed in the risk register found in the appendix. The section below provides a deeper dive into the more significant risks and the corresponding mitigation actions that have been completed or ongoing.

### **City Manager's Office**

#### ***Performance Management Review***

The City Manager's Office routinely reviews departments performance metrics. On a biannual basis the metrics are reviewed and analyzed for performance and to assess whether the metrics are measuring what needs to be measured. These metrics are utilized in a variety of ways by departments and city management such as providing data to substantiate budget requests or to identify how well things are going in each area or to identify areas of concern that are not performing as well.

#### ***Business Plans***

The City had all departments and service areas create and complete business plans. These business plans help strategically align the departments missions and goals to objectives that will be completed over the next few years. The business plans had the departments identify their key performance indicators that tie their strategic goals with City Council Goals. Council goals were also used to tie in and from an action plan created to enhance the department's ability to meet organizational, customer, and workforce requirements. The business plans are utilized by staff as they move forward in completing their action plan.

#### ***Legislative Task Force***

The Legislative Task Force is a special ad hoc group comprised of active leaders in the community - the leadership of City Boards and Commissions. With the membership comprised of the Boards and Commissions leadership, the Legislative Task Force are knowledgeable members of the community, educated on City priorities, and representing a wide range of City interests. The Legislative Task Force will provide input to City Council on the issues relevant to the State Legislative Agenda in preparation for the Texas State Legislative Sessions.

### **Facilities**

#### ***Facility Access Policy***

As City Facilities move to a public lobby and secure back of house model, access control becomes more important. This policy will help establish necessary employee access to non-public areas within City Facilities.

#### ***Georgetown Municipal Complex Remodel***

Secure separation of public and employee space requires building modifications, including access control doors and publicly accessible meeting space to keep employees from bringing public into the secure space. The GMC remodel creates that separation and adds meeting space in the public area.

#### ***Light and Waterworks Remodel***

Light and Waterworks building currently requires entry from an alley and there is no separation from the public space and employee areas. The LWW Remodel moves the front Planning entry to Martin Luther King Jr. St. This entry fits better within the City Center and allows the use of a public lobby with a secure door to the employee area.

## Emergency Management

### ***COVID-19 Response***

The City declared a local disaster and activated a virtual emergency operation center in response to COVID-19. In addition, the City is working closely with Williamson County, the Williamson County and Cities Health District, and State partners to coordinate our response to the pandemic.

In July, the Mayor issued an order requiring the wearing of face coverings while in businesses with some exceptions. These orders were later amended to reflect statewide mask order issued by the Governor. The Governor's orders also prohibit outdoor gatherings of more than 10 people at a time, without mayoral approval.

Additionally, the City is seeking reimbursement through Williamson County for COVID-19 related expense that are eligible to be covered by the CARES act. These funds are being dispersed in three tranches to cover expenses through calendar year 2020. The City has also created an inventory of personal protective equipment to ensure adequate supplies both for first responders and general employees to be appropriately protected.

Finally, the City has amended internal personnel policies to ensure appropriate social distancing at work, allowing employees to telework when appropriate, and appropriate measures are taken when employees test positive for COVID-19, including administering federal ESICK and EFMLA programs.

### ***Hazard Mitigation Action Plan***

The City is in the process of updating its Hazard Mitigation Action Plan. The plan helps the City appropriately assess, prioritize, prepare for, and mitigate natural or human-caused hazards. This plan will allow the City to maintain eligibility for future federal mitigation grant funding and help identify mitigation actions that will make the local community more disaster resistant. The planning efforts are expected to begin in October and be completed in the first quarter of 2021. The plan will require state and federal review prior to City Council adoption.

## Public Safety

### ***HIPAA Audit***

In the spring of 2019, the Fire Department filed a "breach notification" report regarding an unencrypted EMS tablet that went missing from one of the ambulances. This breach had the potential to impact up to 719 individuals and the City began a review of procedures and practices. This review has been expanded to include a HIPAA audit in September 2020 to adequately address any gaps in procedures and policy. The audit will identify measures that need to be taken to maximize the protection of private health information as defined within the Health and Human Services' Security Rule 45 CFR Part 160 and Subparts A and C of Part 164. The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. This audit will help

inform changes that need to be made to reduce the risk of a breach occurring again and is expected to be completed by December 2020.

Also, to further reduce risk, the City is in the process of creating a HIPAA hybrid entity which would create a healthcare component and discern what areas would be subject to HIPAA privacy regulations. This would ensure that only the designated areas that need to comply with HIPAA privacy rules would do so, instead of the entire organization. Only these newly identified areas would have the right to use, maintain, access and/or transmit personal history information. This process will create clear boundaries to further protect sensitive information and create internal controls to limit access.

#### ***Guardian Tracking: Performance Management Software***

Since 2012, the police department has been utilizing Guardian Tracking, a performance management software platform. The software is used to formally capture praise, counseling, goal setting, and discipline. The software also serves as an early warning system for repeated substandard performance.

#### ***Replacement of Police Body Cameras***

In 2019, due to reliability issues with the previous vendor, non-compatibility between car and body cameras, and the inability to keep existing equipment serviceable we replaced all car cameras, body cameras, and facility interview cameras. We transitioned to WatchGuard, a Texas based company and industry leader with regards to police vehicle cameras, body cameras, and digital evidence management software. Now all cameras and the digital data derived are on one unified management software system. The current technology is far superior to the old allowing for real time viewing, wider angles, seamless integration between car and body cameras, and automatic synchronization of all incident cameras on playback.

#### ***CommUNITY Advisory Task Force***

The police department established a Chief's CommUNITY Advisory Task Force in July of 2020 comprised of 20+ diverse community leaders. The task force will be working with the Chief to provide input regarding the state of policing in Georgetown as well as providing input as to the direction of the CommUNITY Initiative. The police department plans to conduct six Listen and Learn Summits across six different stakeholder groups in FY2021.

#### ***Police Training - Arbinger institute***

The police department is in the process of having their officers complete training created by the Arbinger Institute. This training focuses on transitioning a self-focused inward mindset to an impact-focused outward mindset. Arbinger's Policing with an Outward Mindset™ program addresses three key challenges in law enforcement today:

- Situational Awareness and Officer Safety
  - Officers must increasingly operate in ways that are both smart and safe. This requires the self-awareness and motivation to be the most trained, skilled, and conditioned version of themselves possible. In addition, officers must be aware of contextual behavioral anomalies indicative of dangerous or criminal behavior without being distracted by factors such as race, gender, age, sexual orientation, etc.
- Trust and Collaboration

- With so many factors influencing incident narratives and investigations, trust, and collaboration within agencies and with the communities they serve has become critical—but also quite difficult.
- Leadership
  - Law enforcement leaders today must carry a deep sense of personal responsibility to develop competency in each of their roles and to understand the impact they have on others while carrying out their duties. Such a leader inspires and systematically develops similar personal responsibility from others.

Arbinger enables organizations and their people to turn outward through a three-step process: mindset change, leader development, and systems improvement.

STEP 1 Mindset Change	STEP 2 Leader Development	STEP 3 Systems Improvement
<b>OUTWARD MINDSET TRAINING</b> Self Awareness Tools Collaboration Tools Accountability Tools Influence Tools	<b>OUTWARD LEADER TRAINING</b> Role Definition and Goal Setting Tools Performance Conversation Tools Correction and Discipline Tools Conflict Resolution Tools	<b>QUARTERLY IMPLEMENTATION SESSIONS</b> Policy and Procedure Revision Process Improvement Labor-Management Relations Leader Mentoring
<b>8-WEEK SUSTAINMENT PROGRAM</b>	<b>ADVANCED LEADER TRAINING</b>	<b>STRATEGIC PLANNING &amp; EXECUTION</b>
<b>IMPLEMENTATION COACHING</b>	<b>LEADER COACHING</b>	<b>EXECUTIVE COACHING</b>

### ***Fire station 6 and 7***

Fire Station 6 is open and 7 is set to open soon, adding additional resources to key areas within the City for a more efficient response. In having these stations come online the Fire department will also have more staff to reduce the number of overtime hours.

## Finance and Human Resources

### ***Workday***

The City has converted to a new ERP system, Workday. This new system has aligned financials and human resources to one system streamlining purchasing, travel, recruiting, on-boarding, performance, benefits, payroll, accounting, and budget to name a few high-level processes. This conversion has fully mitigated many threats outlined in the 2018 assessment with more restricted security roles limiting access to sensitive information. The system also requires 2-factor authentication furthering our security of the system. Workday is cloud based, allowing for business continuity in the case of a disaster impacting our critical network and infrastructure. Overall, conversion to Workday has allowed for more efficient processes and reporting options for staff.

The workday implementation has addressed the following:



- Conducted detailed process reviews to implement best practices
- Enhanced user and access controls
- Requires 2 Factor Authorization to access
- Created process controls such as budget checks on purchases and created a system of multi-level of approvals for purchases
- Implementing the budget module Adaptive to streamline and integrate workflows within the Workday system

#### ***Internal Audit Plan***

Staff is creating a multi-year internal audit to apply a disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. The internal audit plan reinforces the City's commitment to accountability and integrity while having an objective party look for ways to improve operations. Some of the audits staff are including in the audit plan are:

- Fee Collection Review
- Hotel/Motel Audit
- Franchise Fees
- Airport Revenue

#### ***Sales Tax Audit***

The State is currently conducting a sales tax audit that began in June 2020. The audit is done to ensure that Texas tax laws are applied uniformly and to promote compliance. The audit helps determine whether taxes have been properly collected, reported, and paid to the state.

#### ***Policy Updates***

Six personnel policies were updated in alignment with Workday implementation in 2019 including introductory period, vacations, sick leave, hours of work, compensatory time, and holiday. Multiple temporary policies have been issued during the COVID-19 Pandemic including telework and flex time.

#### ***Safety & Risk Management Team***

The City's safety and risk management programs were combined, centralized, and staffed by three full-time employees focused on the development and evaluation of occupational safety and risk management programs in 2019.

Since that time, the team has improved handling of citizen claims, improved accuracy in covered city property, improved management of our third-party risk pool administrators, and given greater support to our employees who experience work-related injuries.

The team has deployed the first phase of active shooter and building evacuation training, with more to come. They are also building data sets to better understand worker injury and accident trends and working with stakeholders on appropriate mitigating actions.

#### ***Organizational Development***

The City hired its first learning and development coordinator in 2020. The coordinator has built a learning and development strategic plan that will be deployed over the next two years. Included in that plan is our multiyear approach to talent management and making use of Workday talent capabilities.

In 2019 the City created the organizational & operational excellence office, focused on helping staff 'eat elephants...one bite at a time.' The office works to empower staff at all levels through our organizational performance management (see City Manager section) and process improvement programs. The office has since rolled out annual business plans for all departments, lean trainings to over 1,000 participants, and currently support over 60 lean process improvement projects.

## City Secretary

### ***Freedom of Information Act – Compliance with Open Records***

The Open Records Coordinator will continue to provide annual trainings to staff related to best practices for responding to FOIA requests and do routine reviews of the Open Records Request policies and procedures. The City Secretary's Office will continue to work towards adding another Open Records Coordinator to mitigate the large workload that the growing number of open records requests provide.

### ***Records Management – Current Practice***

The Records Management team does routine departmental check-ins and works to organize projects that make departments more efficient and less reliant on paper. The Records Management Team does a routine review of the Records Management policies and procedures to ensure that best practices are always being implemented. They also provide annual training to all employees.

### ***Agenda Process***

Staff members from City Secretary's Office, City Attorney's Office, City Manager's Office, and Purchasing are working together to improve the agenda process that is currently not as efficient as it could be. City Secretary Office is also looking into the possibility of switching agenda software.

## Information Technology

### ***Cybersecurity Policy***

The IT Department has completed a primary draft of a comprehensive Cybersecurity Policy. The draft has been reviewed by first line technical staff and is being prepared for final round of review by the Human Resources, City Secretary, and Legal Departments.

Staff participated in a cybersecurity tabletop exercise in October 2020 conducted by the Texas Department of Information Resources. The tabletop discussion covered the potential impacts of a computer security incident impacting a local community. This training furthered staff's education on responding to a cybersecurity incident and its potential impacts.

### ***System and Network Contingency Plan***

The IT Department currently has an Incident Response Plan in development through the Human Resources Departments Lean Process Development methodology. This plan is scheduled for completion in December of 2020.

### ***Security Information and Event Management System***

Multiple Security Information and Event Management Systems (SIEMs) are under review by the IT Department. Also, the IT Department is evaluating the possibility of managed service contracts through the Texas Department of Information Resources to help fulfill this need. Due to budgetary constraints presented by COVID-19, a purchase was not proposed for FY 2021. Pending budget availability for FY 2022, IT will work toward the purchase and implementation of a SIEM system.

#### ***Staff IT Security and Awareness Training***

The City of Georgetown successfully implemented a Security and Awareness Training initiative in FY 2020. This included training and testing for all City IT users through the City's Learning Management System. In June of 2020, the City Security Awareness Training program was certified by the State of Texas as complete for the current calendar year.

#### ***Back-Up Data Center***

A back-up data center was successfully brought online in the Winter of FY 2020. The purpose of this data center is to act as a failover in the case of a failure at the City's primary data center. Failures could include physical destruction or damage to the primary datacenter by a man-made or natural disaster. Failures may also include some types of cyberattacks. In such a case, the back-up data center could be brought online and subsequently run 90 percent of the City's technology systems within a matter of hours. This includes all the City's mission critical data systems.

### **Overall Utility System**

#### ***Weaver Assessment – Cash Receipt Review***

The City of Georgetown engaged with Weaver and Tidwell, LLP to provide assist in the review and identification of all cash receipts currently received by the City's Utility Billing Office and identify alternative locations and processes for non-utility payments. Weaver and Tidwell also provided risk-control matrices and process mapping for areas in the City's Utility and Accounting Offices where internal risks could occur.

#### ***Weaver Assessment – UMAX Business Process Mapping***

The Weaver and Tidwell, LLP engagement also provided a review of the City's Utility Office internal controls, transactional processing efficiencies and review of audit trails and automated workflows integrated in the City's new UMAX/CIS. Four (4) high-risk, fifteen (15) moderate risk, and four (4) low-risk processes were identified. These ranking provided guidance to the City with regards to prioritizing effort and resources. It also documented workflows that are used when reviewing business processes. The high-risk areas have been mitigated and many of the moderate risks have been addressed.

#### ***Gartner Assessment – AMI/CIS and MDM Systems***

The City of Georgetown engaged with Gartner Consulting to conduct an assessment an analysis of the City's Customer Information System (CIS), Advanced Metering Infrastructure (AMI) and Meter Data Management (MDM) systems. The objective is to evaluate the City's CIS business processes against the current CIS system, identify gaps or areas for opportunities, and explore alternative options to improve the City's CIS operations and supporting technologies. As well as to evaluate the business value provided by the AMI and MDM systems to enable the City to meet its smart meter information needs.

## Electric

The electric utility went through a management assessment conducted by Schneider Engineering., The following were the recommendations from the management assessment:

1. Develop and implement comprehensive risk management policy.
  - a. Leverage internal and external resources to increase oversight and accountability for decision making regarding contracts management.
  - b. Procure third party energy management services.
2. Study the installation of separate governance structure for Georgetown Utility Systems.

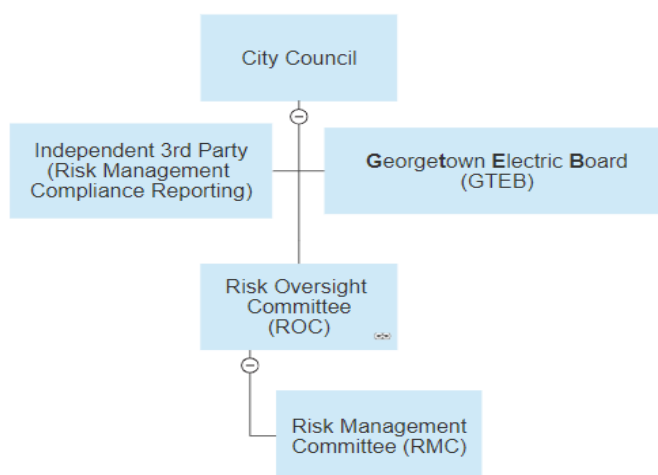
Based on the recommendations, the following action were taken to better manage the risks.

### **Adoption of comprehensive Energy Risk Management Program:**

The new Energy Risk Management Policy governs all purchase power and related activities that may impact the Energy Risk profile of Georgetown Electric Utility. Activities that fall within the scope of this Policy include, but are not limited to, the following:

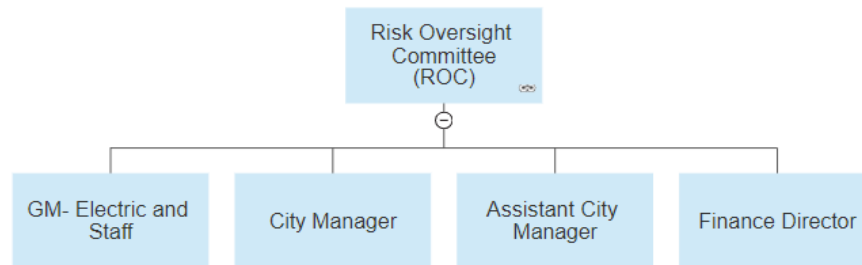
- Wholesale Transactions (PPA, Bilateral Trades)
- Independent System Operator (ISO)/ERCOT Market Transactions (DAM/RTM/AS)
- Energy hedging activities involving physical and financial energy products
- Basis hedging activities involving energy products
- All energy commodity trading
- Counterparty contracting and credit management

Under the new Energy Risk Management Policy there are multiple levels of oversight provided to the electric fund.



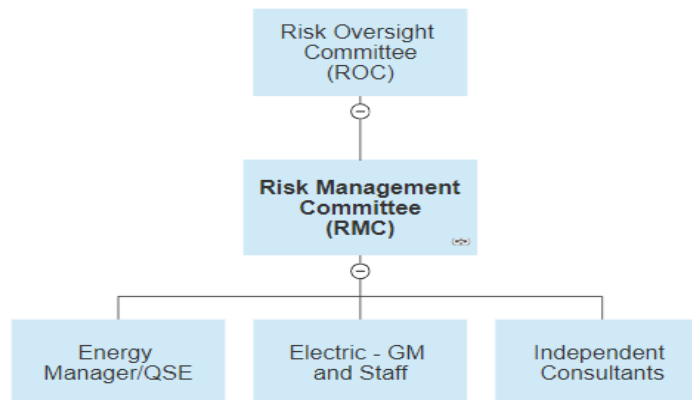
Overall policy oversight is provided by City Council and the Georgetown Electric Board (GTEB). Independent 3rd Party provides Risk Management Compliance reporting to GTEB and City Council.

### ***Risk Oversight Committee***



The Risk Oversight Committee (ROC) is an internal committee that oversees approval and compliance of transactions and risk limits. The committee is comprised of the City's executive team (City Manager and Assistant City Managers), the Electric General Manager and staff, and the Finance Director. ROC provides inputs to the risk management strategy and receives weekly/monthly risk management updates from the Risk Management Committee.

### ***Risk Management Committee***



The Risk management Committee (RMC) is comprised of Shell, the Electric General Manager, and staff, as well as independent consultants. The RMC implement the risk management strategy approved by the ROC. The RMC reviews existing and potential transactions, monitor proximity to limits, and helps support the responsibilities of the ROC. Ultimately the RMC, is responsible for the day-to-day execution and management of transactions.

### **Procurement of 3<sup>rd</sup> Party Electric Energy Portfolio Management Services:**

In December of 2019 Council approved an agreement with Shell Energy North America to provide energy management services. Shell will be developing and making recommendations regarding how Georgetown's energy is traded in the Texas energy market. Shell will also assist in forecasting energy needs, energy costs, and addressing challenges related to transmitting energy around the state, all of which affect the city's costs associated with purchasing power.

In addition to Shell North America, Crescent Power and ACES Power Marketing aid the staff in managing the overall energy portfolio risk and risk management policy compliance.

### **Creation of new Electric Board to provide better risk and financial oversight:**

Starting June 2020, a new electric oversight board was set up. The electric board's proposed role in risk management is as follows:

- Aid the City Council in providing the overall Policy Oversight.
- An independent third party appointed by the Georgetown Electric Board will provide periodic Risk Management Policy Compliance reports to the GTEB and City Council.
- Receives Monthly Risk Management Policy updates from Risk Oversight Committee (ROC) and Risk Management Committee (RMC)

### **Line Extension and Meter Connect Revenue Risk Mitigation**

To ensure all revenue is properly collected, review of the revenue generating activities related to electric infrastructure additions and service provisioning identified revenue loss and revenue leakage.

The causes for lost revenue and revenue leakage were:

1. Unsent/unpaid/overdue invoices for electric infrastructure additions.
2. Sub-optimal business processes and significant short comings of the software systems led to significant under-collection of electric meter connect fees.

Mitigation activities:

1. Business re-organization led to the electric engineering and project management function under the electric cost center. This identified the revenue losses and the redesigned processes led to better control and management of the electric infrastructure additions with appropriate cost recovery.
2. New Electric line extension policy implemented in early part of FY 2020, clearly identifies the infrastructure addition costs and the requirement of pre-payment of the invoices mitigated the risks posed by unpaid/overdue invoices.
3. Short term mitigation strategies were identified which address the meter connect revenue loss. The long-term mitigation strategy of a comprehensive business process redesign of the utility service connection is in progress. The new process will be in place starting January 1<sup>st</sup>, 2021.

## **Water and Wastewater System**

### ***Risk Assessment of Water Utility***

The water utility had a risk and resilience assessment conducted by CDM Smith to comply with a new mandate set by the American Water Infrastructure Act. The assessment outlined several recommendations to help mitigate risks and improve system resiliency against the highest risk threats identified. The recommendations for the water utility system are:

- Plan for use of portable power supply generators during an emergency to supply temporary power to critical system components that do not currently have back-up generators or hook-ups.
- Expand Lake water treatment plant and build a new water treatment plant south of the lake to improve system redundancy during an emergency (this is in the planning process with expansions and new treatment plant construction tentatively scheduled within the next five to seven years).
- Implement floodproofing techniques at the Park water treatment plant to protect critical system components from damages during flood or dam failure.
- Develop a source water protection plan for Lake Georgetown and Lake Stillhouse Hollow in coordination with the Brazos River Authority, United States Army Corps of Engineers, and other stakeholders.
- Improve physical security measures at critical facilities to reduce the risk of an outsider threat accessing critical assets. Examples may include automatic lock doors at water treatment plants, or motion sensors that trigger security camera alerts outside of regular business hours when personnel are not physically on-site.

Many of these recommendations are being addressed in the years to come with the City's capital improvement plan to expand water treatment capability as well as an initiative with the Brazos River Authority (BRA) to secure additional water resources for the future.

### ***Succession Planning***

The Water Utilities Director is set to retire by the end of the year. Upon their departure the water department will lose a vast amount of historical knowledge of the utility and expertise in the field. The City has started a plan to begin a national search for the next water utility director. In the meantime, the director has informally begun to prepare his direct reports to be able to assume more responsibility and is training them on any knowledge gaps he foresees.

### ***Long Term Water Planning***

The city is pursuing several resources when it comes to Long term water planning. Planning is conducted on a State, Regional and local level. The City works closely with neighboring cities, the Brazos River Authority (BRA) and Region G to analyze and develop additional water resources available to meet the City's long-term needs. The BRA and the City of Georgetown are jointly funding and participating in an Aquifer Storage and Recovery (ASR) Study. This study will look at seasonal recharge of surplus reservoir water from Lake Georgetown, treating this water during times when there is spare water treatment capacity and then conveying this water to a suitable location within aquifer(s) that can be used to store the water. During periods of high-water demand or extended drought, the stored water may then be recovered to meet water resource needs. This storage and utilization method may also be used to store additional groundwater resources. The BRA, City of Round Rock and Georgetown are jointly participating in a collaborative study to identify regional and long-term water solutions for Williamson county, the evaluation will include groundwater and conjunctive water development opportunities that have been presented by different marketing groups, water sharing and scenarios for potential redistribution of water

supplies for regional and long-term sustainability of water supplies in Williamson county. James (Jim) Briggs, former Utility General Manager, has worked to include additional groundwater resources from counties to the east as a long-term water resource within the Region G Plan. By having groundwater listed as a long-term solution on the Region G plan, related projects will be eligible for state funding participation.

### ***System Interconnects***

The City is further diversifying its water resources and increasing system resilience through interconnects with neighboring systems. The City currently has two interconnects with Round Rock and a third under design to utilize Round Rock's excess treatment capacity. An additional short-term interconnect is also constructed between the City and Leander's system. This interconnect will be used during periods of high demand. The use excess treatment capacity of others assists the city in being fiscally responsible in the ability to defer capital construction when possible.

### ***Water Leak Detection***

In an effort to more responsibly utilize current water resources the City continues to track and trend Water Loss as a key operating metric. Starting in Fiscal year 2021, the city will be improving leak detection by using satellite detection. The City's vast service area makes this method of detection and subsequent repair more efficient.

### ***Water Rates***

The city continues to maintain utility fiscal health by performing rate study and impact fee studies every three years. Previous rate studies were conducted on a revenue sufficiency principal. The rate study currently is a cost-of-service rate study. The water rates and tiers were evaluated primarily for residential customers and will be in effect 2021. Commercial tiers, and reclaimed use is to be analyzed in 2021. Implementation of the new water rates and narrowed tiers will assist the utility in maintaining financial integrity and make significant effort to improve resource use efficiency.

## **Public Works**

### ***Capital Improvement Project Coordination Committee***

The lack of regularly scheduled CIP Coordination meetings outside of the annual budget process has led to disjointed communication with the CMO on capital improvements projects and, at times, has limited the ability of the organization to consider the full range of options as obstacles, challenges, and opportunities have arisen. All of which is why a new internal committee is being created to enhance CIP coordination across the City. Enhanced CIP coordination will save time, increase accountability, reduce errors, improve timely project close-out, improve debt tracking and issuance, minimize miscommunication, improve intergovernmental coordination, increase accuracy of billing to correct cost centers, and increase opportunity to proactively respond to challenges, obstacles, and opportunities.

### ***Contract Coordinator***

The City of Georgetown hired a contract administrator in March of 2020. This role is responsible for enhancing contract management for various types of agreements, by working with City staff to raise additional awareness for upcoming obligations. Since being hired on the contract administrator has assisted in modifying the internal cover sheet process for two major developments, this improvement led



to identifying over a million dollars in funds owed to the City for public infrastructure. This continuous process and review by the contract administrator will allow for more detailed oversight in the growing number of contracts as the City expands. The contract administrator created a tracking process to monitor the monetary obligations owed to the City or what the city owes given contract specifications.

Also, a Contract Coordination Committee has been formed with its initial meeting scheduled for October 2020. This will further assist the City in working together to track obligations that need to be met. The position will also be the liaison for the City regarding new MUDs and PIDs wishing to be created within City limits and ETJ.

## Near Term Action

- Complete Hazard Mitigation Plan
- Conduct a citywide operational and enterprise risk assessment every 5 years-with the next study slated for FY23
- Implement consultants' recommendations as a result of the following studies:
  - Gartner Assessment of CIS/AMI/MDM systems
  - HIPAA Audit by SHI
- Conduct an audit of the electric risk management practices
- Finalize and initiate internal audit work plan
- Process improvement
  - Streamline purchasing process and create training for power users to ensure compliance with procurement laws
  - Integrated Council agenda process across the City Manager's Office, City Secretary's Office, City Attorney's Office and Purchasing department as well as creating and implementing training for power users on the agenda process
- Overall biannual review and update of citywide and departmental policies and procedures
- Providing public dashboards of departmental performance management metrics

## APPENDIX

### Risk Mitigation Register

RISK REGISTER

RISK LOG										
RISK					ASSESSMENT		RESPONSE			
RISK ID	Risk	DESCRIPTION	Risk Owner	Contact	Residual Risk	MITIGATION STEPS IDENTIFIED	COMPLETED ACTION	NEEDS	RESPONSE STATUS	NEXT STEPS
R01	IT Cybersecurity Governance Model	A comprehensive Information Technology (IT) cybersecurity policy and procedures document has not been approved by management and communicated to all employees and relevant external parties, outlining responsibility and oversight for Information Security (IS) and policy administration.	IT Director	Chris Bryce	21	1) We recommend the City implement a governance framework that allows for the proper management of a successful ISP. An effective ISP involves participation from senior management to set the direction for proper information security practices, adequate staffing and compliance with policies 2) Further, we recommend the City adopt a practice of performing a Cybersecurity risk assessment periodically. The periodic approach may take either of the following approaches: (A) performing a full assessment every other year due to intensive resources required to facilitate such an exercise or, (B) a targeted approach done annually including: <ul style="list-style-type: none"><li>revisiting this report findings and updating controls where appropriate,</li><li>re-assessing the City's mitigation plan to update progress and note any further concerns, and/or,</li><li>selecting a few high-priority control areas (e.g. vendor management, or any business objective/goal identified by executive management) and re-assessing associated threats related to those areas</li></ul>	1) Implementing IT Catalyst Plan – 5 year Strategic Plan 2) Developing documented policies to address various IT areas 3) Developing Cybersecurity Training 4) Conducted 2 security audits 5) Budgeting Lead System Security Analyst in FY19 6) Conducting PCI (Payment Card Industry) study (scheduled) 7) Implementing two factor authentication 8) IT Cybersecurity Risk Assessment by the US Department of Homeland Security 9) Determine best practices, implement security policies, and identify staffing/challenges to implement ISP 10) Identify staffing needs to appropriately manage IT security challenges and ISP 11) Continue Cybersecurity scanning on a yearly basis. 12) Implement ISP 13) Assigned security roles to existing staff and hired any security staff needed to manage an Information Security Program		FULLY MITIGATED	1) The City has completed a draft Cybersecurity policy that is under review by multiple departments. It is a comprehensive policy that establishes basic security guidelines for all aspects of IT services, infrastructure and staff. The policy includes the designation of Cybersecurity officer in IT to lead implementations. Upon acceptance of the policy, multiple PMP measures will be instituted to measure compliance with policy. 2) The City is currently working with a consultant to perform a study of HIPAA related data security. 3) The City has conducted and passed multiple security assessments including those conducted by U.S. Department of Homeland Security.
R02	Utility Market	Exposure to fluctuations in the market price of utilities	General Manager of Electric Utilities	Daniel Bethapudi	18.75	1) Continue to enhance the City's forecasting tools and techniques to increase granularity and improve accuracy. 2) Continue development of a strategy to meet future peak demand growth with distributed generation and storage rather than remote central generation to mitigate exposure to transmission congestion.	1) Shell was hired to forecast and manage purchasing power. Line extension policies and a rate study by NewGen has been conducted to ensure th electric utility is more resilient to a fluctuation in market price. 2) Daniel Bethapudi was hired to oversee the electric utility. 3) Risk Oversight Committee was created and regular reporting to Council		PARTIALLY MITIGATED	

RISK LOG										
RISK					ASSESSMENT		RESPONSE			
RISK ID	Risk	DESCRIPTION	Risk Owner	Contact	Residual Risk	MITIGATION STEPS IDENTIFIED	COMPLETED ACTION	NEEDS	RESPONSE STATUS	NEXT STEPS
R03	IT Asset Management: Data Classification	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	IT Director	Chris Bryce	17	1) The City should consider classifying data within the system based on its criticality and / or sensitivity (NIST SP 800-53 Rev. 4 RA-2). Classification of data will also help drive the above-mentioned information flow enforcement and help define the City's security architecture 2) We recommend the classification of City data to define an appropriate set of protection levels and communication required for special handling Classifications and associated protective controls (including encryption for data at rest and data leak prevention tools) should take into account department needs for sharing or restricting information and the associated business impacts if such data were compromised. Successful data classification in an organization requires a thorough understanding of where the organization's data assets reside and on what applications/devices they are stored. Handling procedures should include details regarding the secure processing, storage, transmission, declassification, and destruction of data.	1) Implementing IT Catalyst Plan – 5 year Strategic Plan 2) Implementing 2 factor authentication with Workday 3) Implementing consistent role based access to CIS and ERP system functions through Workday		PARTIALLY MITIGATED	1) As part of the Cybersecurity Policy under review, a Data Management policy has been created that lays out a multi-department guidelines to classify and manage sensitive data.
R04	IT Access Management	Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	IT Director	Chris Bryce	17	1) A role-based access scheme should be established to ensure consistent application of user access rights within the system. Users should be assigned their base set of access authorizations based on the concept of "Least Privilege Necessary" to perform their role or job function (as defined within their formal job description). Additional access beyond the previously established role-based access scheme should be formally requested, reviewed for conflicts and approved (NIST SP 800-53 Rev. 4 AC-2). Moreover, Management should consider integrating access rights with data classification efforts identified in Appendix B of this report 2) Ensure a process is in place to approve special access requests and timely de-provision access upon notification from HR	1) Roles and access defined in policy and set in Workday. SCADA is being audited by Homeland Security and will see recommendations to mitigate potential risks.		FULLY MITIGATED	1) As a first step in meeting these requirements, the City has established a Cyber Security policy. As sub policy, that policy includes guidelines on access management. Upon acceptance of the policy, IT will begin implementing aspects of the policy pertaining to IT. 2) IT has implemented an approval process in its ticketing systems for both access requests and change control on major systems.
R05	IT Contingency Plan	Loss or inability to continue business due to natural disaster, system capacity or performance issues, interruption in communication, loss or corruption of data, or loss of critical vendors or staff members.	IT Director	Chris Bryce	17	Plante Moran recommends the City conduct and formalize: (1) A Business Impact Analysis (BIA) which identifies and analyzes mission-critical business functions, and then quantifies the impact a loss of those functions would have on the City, and (2) An information system contingency plan to mitigate the risk of critical system and service unavailability. The contingency planning process should occur after a formal Business Impact Analysis (BIA) is conducted, in order to correlate the system with the critical processes and services provided, and based on that information, characterize the consequences of a disruption. Three steps are typically involved in accomplishing the BIA: • Determine mission/business processes and recovery criticality • Identify resource requirements • Identify recovery priorities for system resources	Preparedness committee in partnership with IT		PARTIALLY MITIGATED	The City will conduct this as part of a Business Continuity Plan

RISK LOG										
RISK					ASSESSMENT		RESPONSE			
RISK ID	Risk	DESCRIPTION	Risk Owner	Contact	Residual Risk	MITIGATION STEPS IDENTIFIED	COMPLETED ACTION	NEEDS	RESPONSE STATUS	NEXT STEPS
R06	Segregation of Duties	The Organization fails to adequately segregate roles and tasks between team members	Finance Director	Leigh Wallace	16.43	1) An annual review of user access for all staff members within the City across all programs managed by IT should be performed 2) Departments that have not had an internal control review within the past five years should evaluate the design and effectiveness of their internal controls	Workday ERP system requires role-based security assignments. The Workday ERP system requires 2-factor authentication to access the system.		FULLY MITIGATED	
R07	Legislation	Governmental laws change that impact the organization by financial, operating, strategic or compliance issues.	CMO	David, Laurie, and Wayne	16.36	1) Council and Management should review and closely monitor the status of annexation plans for the City. After the 2020 census, the City will be limited in its ability to perform annexations due to Williamson County's population surpassing 500,000 citizens 2) The City should work with legislators to clarify the impact of harmful legislation including revenue caps and limits on debt financing for infrastructure during the City's period of high growth and should stress the removal of local control restrictions that impact citizens ability to impart changes in their local community	1) Staff reviews annexations and carefully plans in DPRC 2) Focused Advocacy was contracted as a lobbyist for the City to inform the City of developing and implemented legislation and its affects; as well as lobbies in the City's best interest		PARTIALLY MITIGATED	City is creating a Legislative Task Force with representation from the community to inform the City's legislative agenda.
R08	Emergency Notification System Failure (ENSF)	The City's Emergency Notification System fails to alert citizens in the event of an emergency.	Emergency Management Coordinator	Raymond Mejia	13.81	1) The City should communicate Incident Action Plans for large scale events to all parties involved with the event, including the Convention and Visitors Bureau (CVB) 2) Management should inform all departments of the operating procedures related to the ENSF 3) The EMC should develop basic and advanced emergency management training for key stakeholders in the City (Division Managers) and conduct table top and/or practical training exercises that replicate local level emergencies	1) Incident Action Plans are created and shared with needed stakeholders. With COVID-19 Situational Reports and IAP's were created after EOC meetings and shared with stakeholders. 2) 3) Creation of Preparedness Committee which is working on several emergency management deliverables to better prepare the organization as a whole.	1) Work with utilities to map a process flow to send out alerts (e.g. boil water notices)	PARTIALLY MITIGATED	1) Creation of Continuity of Operations Plan 2) Tabletop exercises completed quarterly throughout the year with Directors 3) Create EOC training and emergency management training for staff on the LMS

RISK LOG										
RISK					ASSESSMENT		RESPONSE			
RISK ID	Risk	DESCRIPTION	Risk Owner	Contact	Residual Risk	MITIGATION STEPS IDENTIFIED	COMPLETED ACTION	NEEDS	RESPONSE STATUS	NEXT STEPS
R09	Fraud	Customer, third party, or internal fraud occurs resulting in a significant misappropriation of assets and/ or incorrect financial reporting, or corruption/ kickback schemes.	Controller	Elaine Wilson	13.75	1) The Finance Department should perform more robust reviews of P-Card purchases and consider utilizing software to perform regular audits of P-Cards 2) The Finance Department should perform annual reviews of P-Card users to evaluate whether the all users actually need P-Cards 3) The City should implement a more extensive asset tracking program, utilizing fixed asset tags on assets valued over \$1,000 with consideration of periodic asset audits 4) Vendor Ship-To addresses should be limited to a “drop down” list consisting only of City facilities 5) The City should consider developing a fraud awareness and prevention training program with active participants across all City departments 6) All changes to IT databases deemed to be material should be tracked on an Audit File Log and reviewed by someone without access to the databases	1) A review of all P-card users was performed during the Workday ERP conversion. Cards were added and reduced as necessary across departments. Several departments turned in individual cards used infrequently, and switched to shared cards monitored by a card liaison. The total number of cards remained the same across the City. Travel requests are now audited before the event occurs, in addition to after the event occurs. This has improved accuracy of travel expenses 2) P and T Card review was done this year with the issuance of new cards 3) Some departments are beginning asset management programs 4) Workday limits ship to address options 5) Cash handling training is required for those handling cash 6) Several levels of reviews for changes to IT database and regularly audited and checked for weaknesses by Department of Homeland Security		PARTIALLY MITIGATED	Have regular audits conducted of processes prone or vulnerable to fraud
R10	Health & Safety	Exposure to potentially significant workers' compensation liabilities due to the inability to maintain compliance with applicable health and safety laws and regulations.	HR Director	Tadd Phillips	13.04	Overall, the City has robust health and safety procedures and should consider adding the following: 1) The Library should develop clear policies and procedures on a course of action when a customer, employee, or volunteer is injured at the facility. 2) The City should review the lifeguard policy for pool facility rentals. The City currently does not provide a lifeguard for pool rentals by the Georgetown Independent School District and does not require GISD to provide their own lifeguard. 3) Consider adding an Active Shooter response plan	1) Centralized safety and risk management team as of Oct. 1, 2019 2) GISD and the City are working on an interlocal agreement that will mitigate the safety risks. 3)November and December active shooter and fire safety training at several City facilities		FULLY MITIGATED	

RISK LOG										
RISK					ASSESSMENT		RESPONSE			
RISK ID	Risk	DESCRIPTION	Risk Owner	Contact	Residual Risk	MITIGATION STEPS IDENTIFIED	COMPLETED ACTION	NEEDS	RESPONSE STATUS	NEXT STEPS
R11	IT Incident Response Management	Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events	IT Director	Chris Bryce	12	We recommend the City implement a formal incident response plan including: 1) Provide a roadmap for implementing its incident response capability; 2) Describes the structure and organization of City of Georgetown's incident response capability; 3) Provides a high-level approach for how the incident response capability fits into City of Georgetown as a whole and the overall Family of Companies; 4) Meets the unique requirements of City of Georgetown's mission, size, structure, and functions; 5) Defines reportable incidents as well as requirements and guidelines for external communications and information sharing (e.g., what can be shared with whom, when, and over what channel); 6) Provides metrics for measuring the incident response capability within the organization; 7) Defines the resources and management support needed to effectively maintain and mature an incident response capability; and 8) Is reviewed and approved by senior management	Preparedness committee is developing a hazard mitigation plan that will address these across departments including IT		PARTIALLY MITIGATED	Preparedness committee is developing a hazard mitigation plan that will address these across departments including IT
R12	Utility Outage	The City is unable to respond to mass failures of electrical, water, or sewage outages in a timely manner.	Utility Director	Glenn Dishong	11.89	1) Maintain equipment useful lives schedule and proactively monitor components which have reached their useful lives 2) Perform a vulnerability assessment to judge your preparedness for handling the increased likelihood for power outages	1) Assets are being monitored as well as their useful lives. 2) Risk and vulnerability assessment was conducted.		PARTIALLY MITIGATED	Continuity of operation plan and playbook for utility outage.
R13	Access to Talent	Organization lacks sufficient staffing levels to carry out its routine operations.	HR Director	Tadd Phillips	11.75	1) The City should evaluate positions with required specialized certifications and determine whether entry level staff members can obtain certifications after hire 2) For specialized positions, including, but not limited to, building inspectors, paving foremen, and traffic engineers, the City should conduct an assessment of staffing levels with a 3-year outlook 3) The Fire Department should develop a plan to acquire the necessary EMS personnel talent	1) Several key departments are initializing step programs to promote staff retention and development for more specialized roles. 2) Many departments utilize metrics to gauge staffing needs with an outlook of a few years. 3) Fire continues to study the needed personnel and requests staff in the budget process. FS 6 and 7 will have the adequate staff to operate.		FULLY MITIGATED	Establish a process to identify staffing level needs with a 3-5 year outlook.
R14	Disaster Recovery / Business Continuity Planning	Inability of the organization to continue key business processes during a potential disaster due to lack of sufficient disaster recovery planning and/or execution.	CMO	David, Laurie, and Wayne	11.6	1) The City has inconsistent DR/BCP across the organization. Some departments have a robust plan and others have none. A DR/BCP should be developed for every City department. Each of these department-level plans should then be integrated into a city-wide plan 2) Tabletop disaster recovery simulations should be performed with all City Departments	1) Business plans have been completed by all departments with their budgets for 2021. 2) Emergency management coordinator is developing policies and procedures as well as tabletop exercises; 2) Disaster Preparedness Committee has been created		PARTIALLY MITIGATED	1) Policies and procedures developed, adopted, and training given to all employees. 2) Tabletop exercises completed quarterly throughout the year with Directors 3+L11) Workday is a cloud system, meaning it is accessible anywhere with an internet connection, including mobile devices.

RISK LOG										
RISK					ASSESSMENT		RESPONSE			
RISK ID	Risk	DESCRIPTION	Risk Owner	Contact	Residual Risk	MITIGATION STEPS IDENTIFIED	COMPLETED ACTION	NEEDS	RESPONSE STATUS	NEXT STEPS
R15	Billing for Citizen Services	Citizens are billed incorrect amounts or not billed at all for citizen services	Customer Care Director	Leticia Zavala	11.37	a. The fine schedule for the Municipal Court citations should be restricted to specific users b. All invoices should be created in a single system across the City and remit-to addresses should be limited by a "drop-down" function consisting of only addresses the City accepts payments c. Management should consider a third party revenue recognition study to validate all sources of revenue are complete and accurate across the City operations d. An outside party, Emergicon, reviews billing for EMS incidents as there are various rates depending on citizen's ability to pay. Emergicon also collects funds and this helps reduce the occurrence of billing errors and improves collections. However, Emergicon also writes off funds and there is no reconciliation of EMS revenue to billings. We recommend the City enhance reconciliation controls around billing procedures and perform internal audits of quality control and verification of vendor compliance.	1) AMI/MDM and CIS systems are currently being reviewed by a third party to identify efficiencies and recommend processes to reduce billing inaccuracies as well as other issues with the systems		PARTIALLY MITIGATED	1) Implement changes recommended by Garner's study of the AMI,MDM and CIS system
R16	Composition of Tax Base	Changes in the balance of commercial and residential tax base result in losses of revenue from taxes.	CMO	David, Laurie, and Wayne	10.63	1) The City should communicate potential new commercial and residential development to directly impacted City departments and evaluate how new development would affect each directly impacted department 2) Management should utilize a concentration strategy that is flexible and supported by realistic expectations	1) City can use the Fiscal Impact Model to estimate the cost to serve and its impact on city services with new developments: DPRC also serves as a vehicle to consider new developments and its impact		FULLY MITIGATED	
R17	Grant Obligations	Organization fails to meet grant covenant requirements.	Controller	Elaine Wilson	10.55	1) The City should designate a staff member as a Grant Administrator. This staff member should be responsible for maintaining a repository of all grants being applied for, awarded, contact person, and any required filings associated with each grant. City should require that all Grants be managed through the new Grant Administrator 2) A Grant Status Report should be provided on a periodic basis to the City Manager's office for potential budget considerations	1) Elaine Wilson is the grant administrator and staff does the reporting for grants. Policy created and training is done with departments with active grants. 2) Quarterly Financial Report includes grant report which is validated by Controller.		FULLY MITIGATED	
R18	IT Third Party Roles & Responsibilities	Security roles and responsibilities are not established for all third-party service providers and lack clear contractual obligations for service level agreements and KPI's.	IT Director	Chris Bryce	10	We recommend management take the following actions: 1) Clearly identify the cybersecurity responsibilities to be outlined in the contract with the service provider including roles for identification, response, and recovery procedures 2) Establish Key performance indicators for third-party responsibilities including number of events, data breaches, number of notifications 3) Continuously monitor contract SLA's and established key performance indicators			PARTIALLY MITIGATED	This is a low priority risk as IT infrastructure is managed in-house. As part of the new Cybersecurity Policy under review, a Vendor Access policy will cover basic guidelines for vendors.



RISK LOG										
RISK					ASSESSMENT		RESPONSE			
RISK ID	Risk	DESCRIPTION	Risk Owner	Contact	Residual Risk	MITIGATION STEPS IDENTIFIED	COMPLETED ACTION	NEEDS	RESPONSE STATUS	NEXT STEPS
R19	Vendor Reliance	Any termination of, or adverse change in, the Organization's relationships with its key suppliers, or loss of the supplies in support of one of the organization's key services	Purchasing Manager	Leah Neal	9.81	1) Assign one person the responsibility of monitoring all key vendors to the City 2) Create a subsidiary listing of all key vendors with contract details, SLA's and performance metrics 3) Report back to City Manager when it is determined a vendor may become insolvent or is not meeting SLA's 4) Prior to contract renewal, negotiate with all key vendors to capture volume discounts and preferred pricing 5) Management indicated Garland Power & Light currently reconciles their meter data to the scheduling data and the transaction settlement engine. This could be done in house but would require additional headcount as the process runs 24/7. Management should consider a cost/ benefit study to do this in-house	1) Not realistic, but procurement could have oversight with contract monitors in each department 2) Existing contracts do not have performance measures built-in. Contracts need more specificity to identify indicators of performance. Contract specialist could help in this area to create a standard for contracts moving forward. Performance of contracts should be done more so on the power user level, but processes should be put in place. 5) Gartner study is identifying best practices and gaps with current MDM/CIS system. There is also a multi-department initiative beginning soon that aims to find efficiencies and streamline the meter-to-cash processes		PARTIALLY MITIGATED	1) Create a sole source policy; vendors should not be the ones to verify that they are sole source and a approval process for sole source needs to be created. 2) Create a better process of procurement; often contracts and purchases on the Council agenda have never been reviewed by the purchasing team. Training recommended for staff on procurement process. 3) Contract Review Committee with members from key stakeholders involved (e.g. Purchasing, Legal, CMO, etc.) to follow best practice and keep all parties apprised of contracts within the City
R20	Physical Security	Facilities are not appropriately secured from unauthorized access.	Facilities	Eric Johnson	9	1) Consider taking inventory of all key cards to validate none have been stolen or lost 2) Consider development of physical security training for all personnel regarding safeguarding of assets, restrictive access to high risk areas, etc. The City must support integrity of physical security through the organization with the assistance of the City's Risk Manager 3) Standardize a consistent security plan across all locations appropriate for each facility 4) The City currently monitors physical access to the facility where IT resides to detect and respond to physical security incidents. However, CoG does not review physical access logs periodically	1) Staff is working on this with the police department, and access is monitored for irregularities. 2) New city buildings were built with security in mind, older buildings are being renovated with employee safety as a priority. 3) The safety team in HR & OD is working on creating a safety plan across all facilities; Emergency Response Plan is also available and being updated. 4) The City monitors when an incident occurs or access usage is used out of the normal operating times or pattern usually seen from whomever is accessing the building.		PARTIALLY MITIGATED	1) Create a formal security access policy 2) Conduct safety training or create training in the LMS for threats such as active shooter and natural disaster like a tornado in the area 3) Remodel GMC to have better safety and controlled access for employees

RISK LOG										
RISK					ASSESSMENT		RESPONSE			
RISK ID	Risk	DESCRIPTION	Risk Owner	Contact	Residual Risk	MITIGATION STEPS IDENTIFIED	COMPLETED ACTION	NEEDS	RESPONSE STATUS	NEXT STEPS
R21	IT Critical Security Event Identification	A formal risk event identification process is not in place to identify, classify and resolve security events	IT Director	Chris Bryce	9	1) Identify high risk events that can be alerted from current logging capabilities (NIST SP 80053 Rev. 4 AU-6). Potential high risk events can be discerned through the risk assessment process (NIST SP 800-53 Rev. 4 RA-3), penetration testing, and best practice documentation. Some common threat events include: • Multiple failed login attempts • Elevations in access privileges • Changes to application code • Changes to security settings • Process specific actions 2) Consider alert generation techniques for risky events such as devices that connect to the network without authorization 3) Identified events should be responded to in accordance with the organization's Incident Response Plan	The City's current Cybersecurity Officer and Operations Staff monitor cybersecurity events.		PARTIALLY MITIGATED	When economic conditions allow, IT intends to implement a Security Information and Event Management (SIEM) system for improved monitoring of security events.
R22	IT Security Awareness, Training and Education	Personnel are not informed of potential IT threats to the organization and are unable to respond effectively	IT Director	Chris Bryce	9	1) Rely on end users as the first line of defense to limit exposure to social engineering frauds and threats 2) Consider increasing complexity of password requirements 3) Create a formal IT Awareness training and provide to all employees on a periodic basis 4) Require employees to formally acknowledge in writing that they have read and understand the security awareness training, and that they recognize the ramifications of non-compliance	In FY 20, the City implemented a Security Awareness policy that includes a requirement that all employees conduct Cybersecurity Awareness training.		PARTIALLY MITIGATED	All employees completed this training and will do so annually. The new policy, currently under review, will also require additional training for employees who handle sensitive data.
R23	Fire Department Failure	The Fire Department is not adequately equipped to handle responses to emergencies in the City.	Fire Chief	John Sullivan	8	1) Consider an independent third party evaluation study of the GFD capabilities, response metrics and resource allocations to evaluate if there needs to be changes to the current resource allocation model 2) Consider cooperative agreements with ESD8 and/or contiguous municipalities to elevate synergistic programs (co-located/co-operated) fire stations and boundary drops (enhanced auto-aid). 3) Consider making licensed buildings be required to be inspected annually. Also, consider a self inspection program for low risk properties and/or an inspection matrix as follows: • Low Risk – every 3 years • Medium Risk – every 2 years • High Risk – annually 4) Management should consider the implications for property owners and businesses when the Public Protection Classification (PPC) issued by the Insurance Services Organization (ISO) is not performed, as there may be a negative impact if not inspected annually.	1) Hired technical advisory: Community risk assessment and strategic plan for accreditation Spring 2021. 2) Finalized a 10 year contract: ESD 3& 5 auto-aid with Williamson, Travis, and Round Rock. Fire station 6 is now open in ESD8. 3) Not needed at this time.	1) Fire Marshall 2) Fire Protection Engineer	PARTIALLY MITIGATED	
R24	Freedom of Information Act (FOIA)	Non-compliance with FOIA requests	City Secretary	Robyn Densmore	6.22	1) When the transfer of FOIA request process is complete, consider documenting the process with written policies and procedures	FOIA policy and procedure created and presented to Directors. City has a full time open records specialist.	Additional open records specialist due to the continued increase in volume of open records requests.	FULLY MITIGATED	Continue annual staff trainings on open records requests

RISK LOG										
RISK					ASSESSMENT		RESPONSE			
RISK ID	Risk	DESCRIPTION	Risk Owner	Contact	Residual Risk	MITIGATION STEPS IDENTIFIED	COMPLETED ACTION	NEEDS	RESPONSE STATUS	NEXT STEPS
R25	Police Failure	The Police Department is inadequately equipped to respond to emergencies or responds in an unauthorized manner.	Police Chief	Wayne Nero	6	1) Develop the following Key Risk Indicators (KRI's) and monitoring controls which may indicate a risk event is about to occur a. Increase in City crime rates b. Increase in police misconduct/brutality incident claims c. Increase in squad car accidents d. Excessive overtime e. Unexpected cost overruns/continuous unfavorable budget variances f. Increase in dismissed cases due to insufficient evidence, improper procedures or failure to follow legal standards for police	1) Metrics for monitoring are closely monitored for trends and shared with CMO and Council. These metrics guide decisions made by the Police chief. B.) Every incident is reviewed/investigated, monthly management report reviewed, and guardian tracking has an early warning system for personnel exhibiting certain performance indicators that triggers higher level review of officer C.) Reviewed and investigated and included in monthly mismanagement report and added to officers file for tracking of patterns. D.) OT monitored every pay period with various measures and historical reviewed E. Costs tracked internally and in workday		FULLY MITIGATED	
R26	Talent Management	Organization lacks a clear assessment and evaluation process to align qualified employees with specific business requirements and needs.	HR Director	Tadd Phillips	5.42	1) Have HR department work collaboratively with business lines to gain in depth knowledge of resource needs and constraints 2) Consider using an outside party for diversity in pre-hire assessments	1. Directors oversee their departments and align those best qualified to fill gaps in their organization through promotion or lateral shifts.		FULLY MITIGATED	Learning and development survey was conducted , city staff were asked to identify their needs for professional development.
R27	Records Management	No records management policy is in place, adhered to, or is inadequately designed.	Records Program Manager	Cynthia Conomos	5.27	1) Formalize Records Management policy regarding digital records and communicate to all departments 2) Consider additional training on electronic records management 3) Consider digitizing Parks & Recreation forms	1) Records management program has an existing policy from 2015, revised in 2019. Team is currently in the process of their records management survey. 2) Began a finance electronic record cleanup to help clear records that met retention and organize files for Finance. 3) Digitizing forms in progress	Records specialist to maintain with the rate of new requests	FULLY MITIGATED	Records team is working with all departments on their records retention program and conducting training.

RISK LOG										
RISK					ASSESSMENT		RESPONSE			
RISK ID	Risk	DESCRIPTION	Risk Owner	Contact	Residual Risk	MITIGATION STEPS IDENTIFIED	COMPLETED ACTION	NEEDS	RESPONSE STATUS	NEXT STEPS
R28	Regulatory Filings	Failure to comply with regulatory filings such as GASB, EPA, etc.	Controller	Elaine Wilson	5.2	1) Agency (EPA) and Texas Commission on Environmental Quality (TCEQ) permit reports every 3-5 years 2) Finance prepares annual CAFR and SEFA which is submitted to the clearinghouse 3) Customer Care prepares annual filings on storm water use survey breaking out how much water was taken in to the system. 4) City of Georgetown has an exemption from complying and filing necessary reports mandated by Senate Bill 898 (reducing energy consumption in City owned facilities) & administered via the State Energy Conservation Offices (SECO) because of the 100% renewable designation. 5) Customer Care is required by TCEQ to report water quality testing results to customers on an annual basis. Deadline for customer communications is 7/1. GUS must certify with TCEQ by 5/1 that we provided water quality testing results to water purveyors that obtain wholesale water from GUS. 6) Energy Services relies on outsource provider Snyder Engineering for all regulatory findings 7) Utility services is subject to an annual requirement with the ERCOT to validate that a risk management plan is in place 8) Airport has a significant amount of regulatory filings ranging from EPA, TCEQ, Stormwater, Airplane inventory, and Property Taxes through MCAT. Use Microsoft Outlook as reminders 9) Fire Dept. has numerous state health services filings regarding training, certifications, incidents, fatalities, etc.	1) Each department is responsible for compliance at the state and federal level and they do so regularly to comply with deadlines.		FULLY MITIGATED	
R29	Succession Planning	Leadership talent within the organization is insufficiently developed to provide for orderly succession in the future.	HR Director	Tadd Phillips	4.39	1) The City should consider an outside party to implement a formal Succession Plan 2) Consider a mentor shadowing program to protect the City against unplanned terminations or leaves of absences	1) Engaged leaders program allows for leadership development. Directors informally plan succession by training assistant directors or identifying d individuals they believe might be right for the job. National searches are done externally to also fill roles with the best candidate. 2) City is establish its organizational development department within HR which will facilitate the creation of programs that will bolster professional development and any other needs of staff identified in the City-wide needs assessment.		PARTIALLY MITIGATED	Learning and development survey was conducted , city staff were asked to identify their needs for professional development. Several departments have incorporated cross-training and succession planning into their operations.

RISK LOG										
RISK					ASSESSMENT		RESPONSE			
RISK ID	Risk	DESCRIPTION	Risk Owner	Contact	Residual Risk	MITIGATION STEPS IDENTIFIED	COMPLETED ACTION	NEEDS	RESPONSE STATUS	NEXT STEPS
R30	Budget and Planning	Budgets and business plans are not realistic, based on appropriate assumptions, based on cost drivers and performance measures, accepted by key managers, or useful or used as a monitoring tool.	Finance Director	Leigh Wallace	3.24	1) Certain departments such as utilities, water, electric, etc. count on supplemental data to prepare their budget (see Data Governance risk #27). We recommend management validate and document the completeness and accuracy of assumptions for all budget line items 2) Management should set a clearly defined threshold for all material variances to be explained (e.g. +/-XX% and \$YY,YYY)	1. New business plans were developed tying KPI's with the goals of that department and the mission. 2. Budget process requires several reviews and checks by analysts and executives to ensure budget lines are appropriate.	The budget development module of the Workday ERP system is currently being implemented. Finance participates in the rate studies and supplemental consultant financial models for the utilities.	PARTIALLY MITIGATED	1) Create a budget with a more detailed 5 year outlook
R31	Tax	Non-compliance with state or federal tax law.	Controller	Elaine Wilson	3	1) Consider the creation of a master tax filing schedule and reporting to City Manager	N/A		NOT MITIGATED	1) Create master tax filing schedule after Workday implementation
R32	State/Federal Regulations	Failure to comply with new or existing federal or state regulations.	Controller	Elaine Wilson	2.44	1) Develop a Citywide license and CPE tracking system 2) Develop a process to ensure all City playgrounds comply with ASTM F1487-07. The code does not require a formal inspections process, just that the City complies with the ASTM F1487-07 standard	1) Workday has capability to track development and performance, but is not being used as the city develops it learning and development program 2) City utilizes third party's to design and construct playgrounds who are aware of state and federal regulations		PARTIALLY MITIGATED	1) Consider tracking CPE's through Workday
R33	Leadership	The people responsible for the important City processes do not or cannot provide the leadership, vision, and support necessary to help employees be effective and successful in their jobs.	CMO	David, Laurie, and Wayne	2.42	1) The City should consider an upward feedback program to validate lower levels of employees are satisfied with management's performance	1) Currently focused feedbacks are in place which are a two-way feedback of the employee and supervisor: Supervisors are evaluated in 360 evaluations by peers; employee engagement surveys are done bi-annually and provide a feedback mechanism as well anonymously 2) More regular feedback is encouraged with the use of the Diamond Drop program		FULLY MITIGATED	

REGISTER DROPDOWN KEYS			
IMPACT / OCCURRENCE LIKELIHOOD LEVEL	HIGH	MEDIUM	LOW
2018 Risks	5	17	11
MITIGATION STATUS	Fully Mitigated	Partially Mitigated	Not Mitigated
TOTAL	13	19	1

IMPACT / OCCURRENCE LIKELIHOOD LEVEL	2018 Risks	Fully Mitigated	Partially Mitigated	Not Mitigated
HIGH	5	2	3	0
MEDIUM	17	5	12	0
LOW	11	6	4	1
Total	33	39%	58%	3%

# Make the mark.

CITY OF GEORGETOWN, TEXAS  
SEPTEMBER 25, 2018

---

Citywide Risk Assessment  
Results & Next Steps



plante moran | Audit. Tax. Consulting.  
Wealth Management.

September 25, 2018

Mr. David Morgan, City Manager  
City of Georgetown  
113 E. 8<sup>th</sup> Street  
Georgetown, Texas 78627

Dear David,

We have performed the procedures as agreed upon in our consultation agreement dated November 7, 2017. Those procedures were applied solely to provide consulting services to assist City of Georgetown, Texas ("City") in developing a Citywide Risk Assessment (CRA) to understand the risk environment and internal control structure of your functional areas and processes to identify key risks and the internal controls over those risks.

The results of this report contain our assessment of the key risks to your organization, rankings of current mitigation strategies, treatment plans to assist in the management of key risks, and emerging best practices in government industry control environments.

We were not engaged to, and did not perform an examination, the objective of which would be the expression of an opinion of City of Georgetown, Texas's internal control environment. Accordingly, we do not express such an opinion. We were not engaged to perform any specific internal control testing procedures beyond inquiry of management and, therefore, we have not done so. Had we performed additional procedures, other matters might have come to our attention that would have been reported to you.

This report is solely for the information and use of the management of City of Georgetown, Texas and is not intended to be, and should not be, used by anyone other than the specified party.

We would like to recognize and thank the staff of City of Georgetown, Texas for the cooperation and courtesy extended to us throughout this process.

Sincerely,

Doug Farmer, CICA  
Partner – Risk & Accounting Advisory Services  
Plante Moran, PLLC

# Table of Contents

Executive Summary	1
Project Scope and Approach	3
Risk Universe	4
Impact and Likelihood Criteria	5
Risk Assessment Results and Next Steps	7
Appendix A: Risk Treatment Action Plans	11
Appendix B: Information Technology Detail	40



## Executive Summary

---

### Purpose and Introduction

In 2017, staff updated the City's Fiscal and Budgetary Policies to enhance the existing internal audit and risk program. The General Government and Finance Advisory Board and the Council added ongoing funding to the Finance Administration budget to support this change. As a first step in the program, the City procured a firm to perform a comprehensive risk assessment. The outcome of the assessment will be used to prioritize the steps to continue enhancing the audit program and mitigating risk.

Plante Moran performed a Citywide Risk Assessment (CRA) of the City of Georgetown, Texas ("Georgetown", "COG" or "City") with the objective of helping the City achieve its strategic priorities and advance management's process to identify, classify and mitigate risks to the organization. Our CRA services consisted of the following:

1. Interview key stakeholders to understand Georgetown's viewpoint on risk management
2. Conduct interviews with key City Departments to assess inherent and residual risks of the risk universe
3. Assess the strength of Georgetown's mitigating activities and risk treatment factors
4. Assignment of risk owners and actions steps for remediation plans, if necessary
5. Preparation of reports to management and Council detailing the results of our work and recommendations to manage risk and strengthen the control environment

### High Level Themes Noted:

- The City is exposed to four high Information Technology (IT) residual risks. We recognize the City is currently in process of an ERP system upgrade and the status of these conditions will change in the near future: IT Cybersecurity, IT Asset Management: Data Classification, IT Access Management and IT Contingency Plan. See Appendix B for IT Risk Report.
- The City lacks a clear process for the assignment and review of user access roles and responsibilities to achieve segregation of duties in three key business departments. We noted during discussions with Finance, Customer Care and Parks and Recreation one person can control more than two phases of a transaction exposing the City to unauthorized transactions and fraud risk.
- Management indicated several potential costly Texas legislative acts are due for review at future legislative sessions.
- The Georgetown Utility Service (GUS) electricity is a vertically integrated monopoly which is allowed in the State of Texas. The Texas Legislature granted an exception called OPT OUT of bundled services and this gets reviewed at each legislative session every two years. If this OPT OUT provision is rescinded, the City would still have the wires/ transmission equipment and would be the whole seller to the power companies but there would be significant effort and expense to the City to be OPT IN ready if the legislature changes position and the resulting transition would take about 2 years.
- The City is challenged with documentation of operating policies and procedures. Currently, 15 out of 25 (60%) departments we interviewed have a lack of clearly written policies and procedures available to all employees.

## Project Approach and Scope

### Approach

We met with management to develop the following:

- **Planning Meeting** – This segment was dedicated to understanding the risks to key individuals in the organization. We worked with management to outline the risks impacting the City.
- **Ranking Criteria** – Based on our conversations with key individuals, we created impact and likelihood criteria for grading / assessment of the risks.
- **Risk Assessment Interviews** - We held risk assessment interviews with key individuals from key departments across the City to capture management's view of inherent risks and mitigating activities.
- **Control Gaps & Observations** – Using the information gained in the items above, we noted observations, identified the top residual risks to the organization, and offered recommendations for control and process improvements.

### Scope

In context of this risk assessment, a “Key Business Department (KBD)” is defined as a vital business process, function or activity on which the organization spends a significant amount of financial or personnel resources to perform, or an activity over which they have primary responsibility within the City. The following 25 departments are considered KPD's and in scope for this engagement:

Key Business Departments (KBD) Listing	
1. (AIR) Airport	14. (GUS) Georgetown Electric / (NRG) Energy Services
2. (ASV) Animal Services	15. (PLH) Planning/Housing
3. (ATT) City Attorney	16. (HUR) Human Resources
4. (COD) Code Enforcement	17. (BINS) Building Inspection Services
5. (COM) Communications	18. (ITS) Information Technology Services
6. (CRT) Municipal Court	19. (LIB) Library
7. (CUS) Customer Care / Conservation	20. (MGR) City Manager's Office
8. (CVB) Convention & Visitor's Bureau	21. (PKR) Park & Rec
9. (ECO) Economic Development / Main Street	22. (SEC) Secretary / Records
10. (ENG) GUS Systems Engineering / GIS	23. (SWR) Solid Waste & Recycling
11. (FIN) Finance, Purchasing & Payroll	24. (TSP) Transportation
12. (GFD) Georgetown Fire Department	25. (WSV) Water Services
13. (GPD) Georgetown Police Department	

Plante Moran met with the department heads and key managers to discuss the risk universe, assess the inherent risks and document the key internal controls and mitigation strategies for each risk in the risk universe applicable to each department. Residual risk scores are calculated based on inherent risk minus strength of mitigation activities.

## Risk Universe

A planning meeting was held with the City Manager and Assistant City Managers to co-develop a risk universe using a standard governmental entity risk profile customized to the Georgetown specifics for population, demographics, services offered, operations and complexity. The initial universe started with approximately 90 risks and the list was distilled down to the top 33 risks applicable to the City of Georgetown. We then met with each department individually to discuss the impact and likelihood to their department. It is important to note that not all 33 risks are applicable to every department. Only 14 out of 33 risks were determined to be citywide impacting all departments. The illustration below is the risk universe utilized for this assessment:

City of Georgetown Risk Universe	
1. <b>Access to Talent</b>	18. IT Security Awareness, Training and Education
2. Billing for Citizen Services	19. IT Third Party Roles & Responsibilities
3. <b>Budget and Planning</b>	20. <b>Leadership</b>
4. Composition of Tax Base	21. <b>Legislation</b>
5. <b>Disaster Recovery / Business Continuity</b>	22. <b>Physical Security</b>
6. Emergency Notification System Failure	23. Police Failure
7. Fire Department Failure	24. <b>Records Management</b>
8. <b>Freedom of Information Act (FOIA)</b>	25. Regulatory Filings
9. <b>Fraud</b>	26. <b>Segregation of Duties</b>
10. Grant Obligations	27. State-Fed Regulations
11. Health & Safety	28. <b>Succession Planning</b>
12. <b>IT Access Management</b>	29. <b>Talent Management</b>
13. IT Asset Management: Data Classification	30. Tax
14. IT Contingency Plan	31. Utility Market
15. IT Critical Security Event Identification	32. Utility Outage
16. IT Cybersecurity Governance Model	33. <b>Vendor Reliance</b>
17. IT Incident Response Management	

Note: the 14 bold risks were common citywide across all departments. The remaining risks were assessed on a case-by-case scenario by department. Information Technology risks were evaluated in three categories: 1) Centrally Managed, 2) Vendor Managed, and 3) Department Managed.

## Impact and Likelihood Criteria

Key department personnel participated in the risk interviews to rank the risks to the organization using an impact and likelihood criteria developed with senior management. The impact and likelihood criteria table below is applied to each risk to assign the inherent risk. The inherent risk rankings are then used as the starting point to calculate residual risks.

Impact Criteria					
Ranking	5 (high)	4	3	2	1 (low)
<b>Financial Impact:</b>					
Expense or Lost Revenue	>\$150K	\$100K - 150K	\$50K - \$100K	\$25K - \$50K	<\$25K
<b>or Strategic Impact:</b>					

Strategy/ Mission/ Legislature	Failure to meet key strategic objective	Major impact on strategic objective	Moderate impact on strategy	Minor impact on strategy	No impact on strategy
<b>or Operational Impact:</b>					
Reputation	Extreme	Severe	Moderate	Low	None
Process / System Shutdown	> 7 Days	5 - 7 days	3 - 5 days	1 - 3 days	< 1 day
<b>Compliance Impact:</b>					
Regulatory - State/ Local/ HIPAA/ Debt Covenants	Large-scale material breach of regulation	Material breach but cannot be rectified	Material breach which can be readily rectified	Minimal breach which cannot be rectified	Minimal breach which can be readily rectified
<i>Likelihood Criteria</i>					
<b>Ranking</b>	<b>5 (high)</b>	<b>4</b>	<b>3</b>	<b>2</b>	<b>1 (low)</b>
<b>Probability of an event occurring in a given year:</b>					
	>20%	15 - 20%	10 - 15%	5 - 10%	<5%
<b>or Event Occurrence (on average):</b>					
	Once a year or more	1 in 3 years	1 in 5 years	1 in 7 years	1 in 10 years

## Risk Identification and Ratings

It is important to clarify the factors in determining the levels of risk as presented in the following departmental risk assessment graphs. For comparability purposes, risk is evaluated by distinguishing between types of risk and the following definitions are provided:

**INHERENT RISK** – the perceived impact and likelihood associated with a process or activity that exists simply from the perspective of its current environment BEFORE consideration of mitigating activities such as insurance, internal controls or other risk treatment strategies. This assumes no significant actions taken by management to mitigate (address) those risks. For example, the City has inherent risks associated with its citizen demographics, funding sources, population, economic slowdown, structure of federal and state government, etc. This can then begin to be refined to the departments within the City government.

**RESIDUAL RISK** – the level of impact and likelihood of an adverse event occurring to impede the City, Department, and/or Processes from achieving success AFTER identifying and testing of management's mitigating activities and internal control structure.

The citywide risk assessment considered primarily inherent risks, with limited identification of control risk as self-reported by management. We did not substantively test specific management controls in detail and therefore, do not render an opinion on the effectiveness of design nor the efficiency in implementation or existence. The ratings do not imply a judgment on how management is addressing risk and thus is not a specific assessment of management performance nor concludes on 'Residual Risk'. Management will need to perform detail testing to determine: (1) if mitigation activities reported by management are actually in place, and (2) if the mitigation activities are designed and operating effectively.

**VELOCITY** – the speed assessment of how quickly a risk will impact the organization:

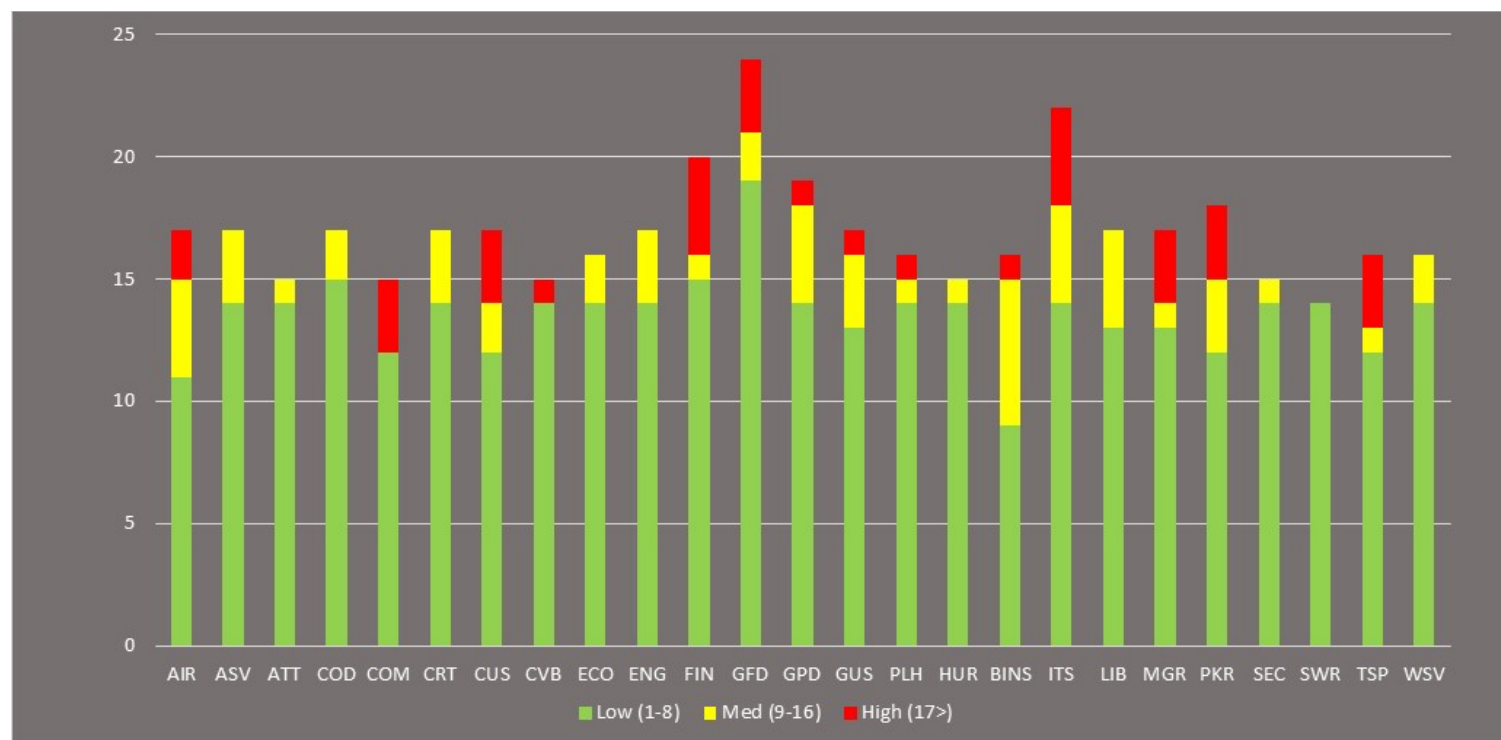
- **Fast:** These risks are becoming more relevant to Georgetown's operations and can quickly impact the organization. Risks with a moderate to high residual risk ranking and fast velocity should be closely monitored as a risk event could occur quickly and without warning.
- **Moderate:** No known or pending events suggest either an increase or decrease in the composite risk weighting. These risks will impact the organization at neither a fast nor a slow pace.
- **Slow:** These risks will impact the organization over time and might require a playbook that extends over a longer period of time.

## Risk Assessment Results and Next Steps

---

The following pages summarize the Risk Assessment Results from 3 different perspectives:

Graph 1 - Net Risks by KBD <sup>1</sup>:



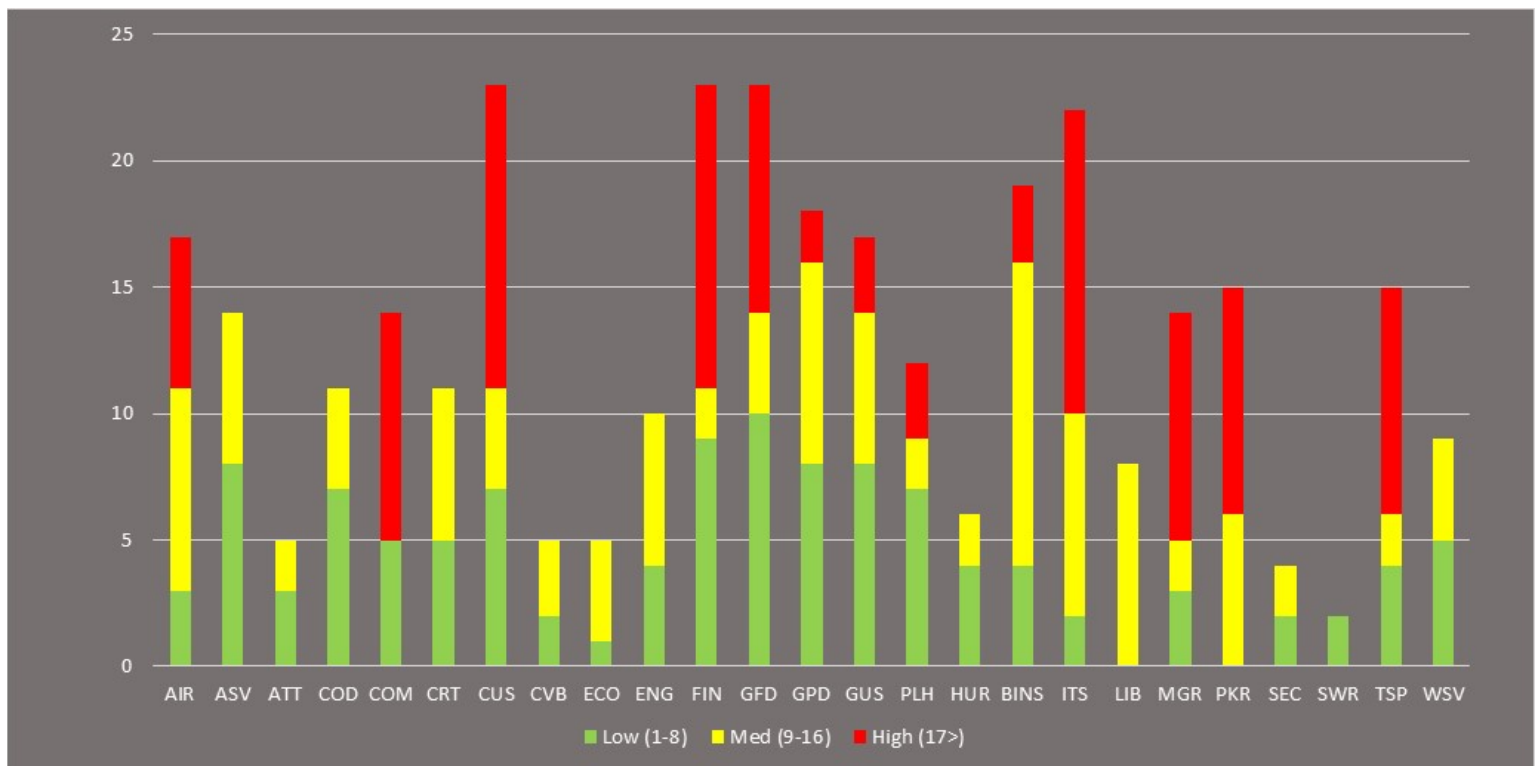
(i) **Net Risks by Key Business Departments:** the total number of risks from the Risk Universe that apply to each department. As noted earlier, 14 of the 33 risks have been identified as pervasive across all departments and the others are assessed on a case-by-case scenario.

The net risk assessment by KBD revealed that Georgetown Fire Department, Information Technology Service<sup>2</sup>, Finance, Georgetown Police Department and Parks & Recreation fall within the high risk category based on Net Risks by Department.

<sup>1</sup> Each department was assessed for the 33 risks outlined in the Risk Universe on p. 3. There are 14 risks that are pervasive across the City and the remaining risks were assessed on a case-by-case scenario.

<sup>2</sup> For the purposes of risk ranking, certain Information Technology risks with similar mitigation activities and control objectives were combined for reporting purposes. The Risk Universe shows 8 IT risks and the detail IT Risk Assessment report is included in Appendix B has 11 risks.

Graph 2 – Weighted Residual Risks by KBD:

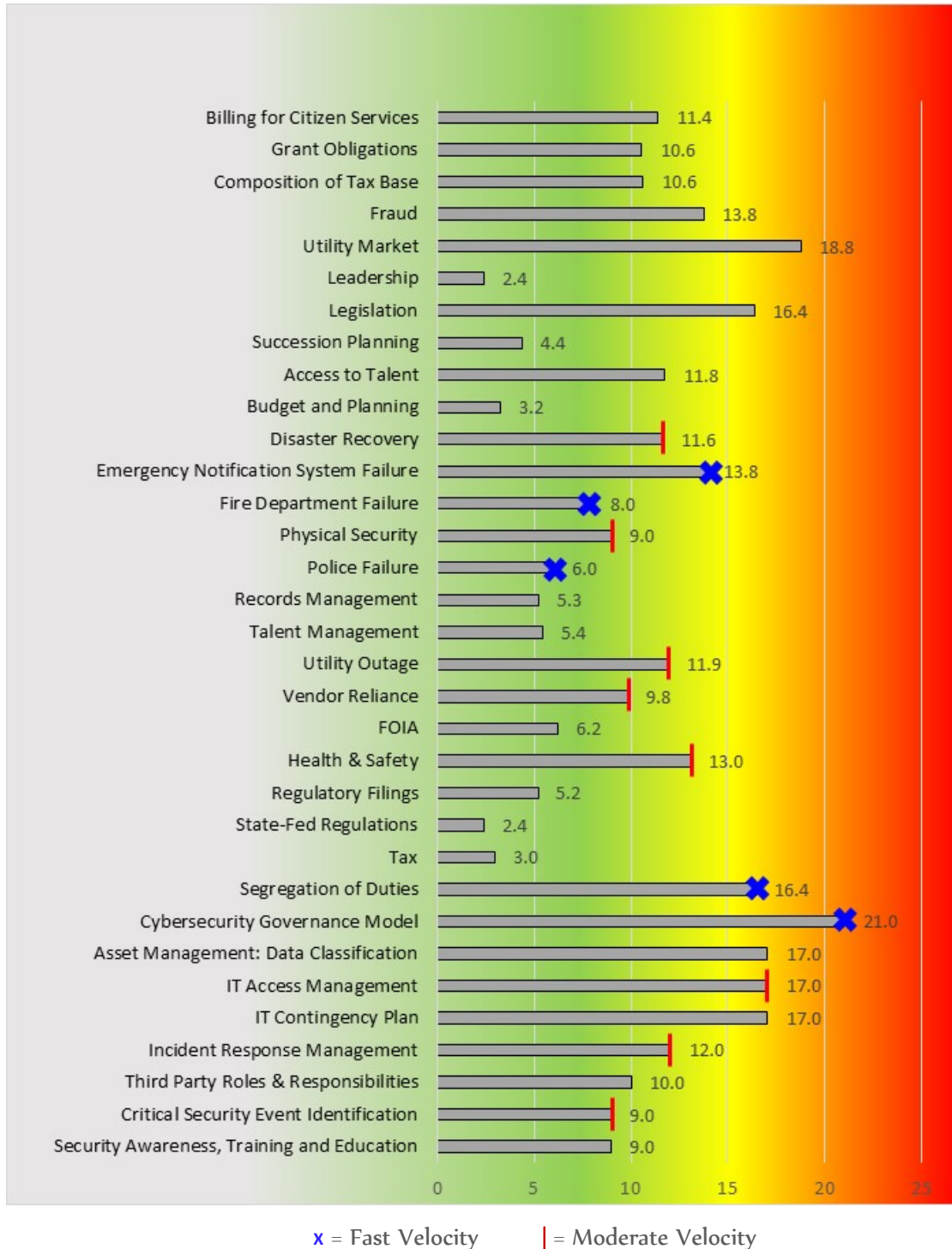


**(2) Weighted Risks by Key Business Departments:** the total number of risks weighted by rankings using the following weighting formula: Red 17 or > (3 points), Yellow 8-16 (2 points), and Green <8 to 5 (1 point), <4 (0 points). Therefore, the higher risk rankings carry a higher weighted risk.

The Weighted Residual Risk by KBD reveals there are two (2) additional departments needing consideration as the ratio of high risks to total brings the residual risk to a high for Customer Service and Building Inspection Services, in addition to the KBD's noted in Graph 1.

Evaluation of these various factors provides indicators on prioritizing the potential Future State Risk Mitigation Activity recommendations outlined in Appendix A.

### Graph 3 – Citywide Composite Residual Risk Rankings



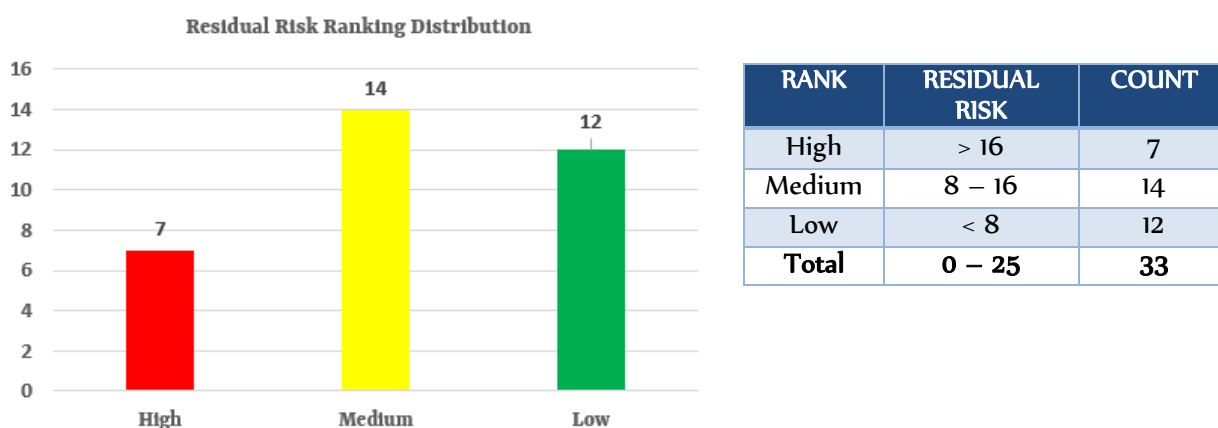
(3) **City-wide Composite Residual Risk Rankings:** the profile of consolidated highest ranking risks to the City regardless of KBD. As noted earlier, certain risks may only apply to a limited number of KBD and may be insignificant on a City-wide basis.



Composite scores represent a cross-section view of risk without regard to KBD. The composite scores above are an average of the risk rankings for only the departments where the risks are applicable. For example, Billing for Citizen Services is a risk to the City but only applies to 13 out of 25 KBD's. The scores above are an average of those applicable departments excluding the departments that do not do billing. Results from this graph illustrate the severity of risk regardless of the department which they fall under.

### Residual Risk Dispersion

The following graph depicts the dispersion of the risk events between high, medium, and low residual risk (including the consideration of existing control or mitigation activities) categories. High indicates that the residual risk score fell beyond Georgetown's risk tolerance. These risks require the most attention and strongest mitigation strategies. Medium indicates that the residual risk was within tolerance. Low indicates that the risk fell well below Georgetown's tolerance. It may be possible that some of these risks are being over mitigated.



### Next Steps

1. Strengthen and implement mitigating activities for each risk to bring the residual risk down into tolerance (see Risk Treatment Action Plans in Appendix A).
2. Assign risk owners and control owners and determine what information needs to be reported back to the City Manager on a periodic basis (i.e., quarterly).
3. Identify a risk management resource to manage the risk owners and communicate all necessary information from the risk owners to the City Manager and City Council.
4. Risk Owners identify key risk indicators (KRI's) for each risk.
5. Build execution playbooks for each risk treatment.

## APPENDIX A – RISK TREATMENT ACTION PLANS



## APPENDIX A – RISK TREATMENT ACTION PLANS

#	Risk	Risk Detail	Residual Risk Score	Risk Owner	Current State Mitigating Activities	Future State Mitigating Activities	Management Response
1	IT Cybersecurity Governance Model	A comprehensive Information Technology (IT) cybersecurity policy and procedures document has not been approved by management and communicated to all employees and relevant external parties, outlining responsibility and oversight for Information Security (IS) and policy administration.	21.00	IT Director	<ol style="list-style-type: none"> <li>1) The City has a documented IT Acceptable Use Policy in place but it does not encompass an overall Information Security Program (ISP) containing the following elements: Purpose/Scope, Roles and responsibilities (including those related to regulatory requirements), Enforcement, Information Sharing, Data Classification, Information Risk Management (IRM), Data Backup and Retention, Data Destruction/ Retention Policy</li> <li>2) Members of the IT department perform several duties beyond their originally assigned tasks and roles and responsibilities related to key initiatives such as Risk &amp; Incident Management, Disaster Recovery &amp; Business Continuity are not clearly defined</li> <li>3) The IT department has taken measures in implementing security practices throughout the IS environment; however organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad hoc/reactive manner; a citywide approach to managing cybersecurity risk has not been established</li> </ol>	<ol style="list-style-type: none"> <li>1) We recommend the City implement a governance framework that allows for the proper management of a successful ISP. An effective ISP involves participation from senior management to set the direction for proper information security practices, adequate staffing and compliance with policies</li> <li>2) Further, we recommend the City adopt a practice of performing a Cybersecurity risk assessment periodically. The periodic approach may take either of the following approaches: (A) performing a full assessment every other year due to intensive resources required to facilitate such an exercise or, (B) a targeted approach done annually including: <ul style="list-style-type: none"> <li>• revisiting this report findings and updating controls where appropriate,</li> <li>• re-assessing the City's mitigation plan to update progress and note any further concerns, and/or,</li> <li>• selecting a few high-priority control areas (e.g. vendor management, or any business objective/goal identified by executive management) and re-assessing associated threats related to those areas</li> </ul> </li> </ol>	<p>The City is already taking several steps to comprehensively manage and enhance security:</p> <ol style="list-style-type: none"> <li>1) Implementing IT Catalyst Plan – 5 year Strategic Plan</li> <li>2) Developing documented policies to address various IT areas</li> <li>3) Developing Cybersecurity Training</li> <li>4) Conducted 2 security audits</li> <li>5) Budgeting Lead System Security Analyst in FY19</li> <li>6) Conducting PCI (Payment Card Industry) study</li> <li>7) Implementing two factor authentication</li> </ol> <p>IT agrees that an Information Security Program (ISP) needs to be created.</p> <p><b>IT Immediate actions</b> <i>(next 12 months)</i></p> <ol style="list-style-type: none"> <li>1. IT Cybersecurity Risk Assessment by the US Department of Homeland Security. 2. Determine best practices, implement security policies, and identify staffing/challenges to implement ISP. 3. Identify staffing needs to appropriately manage IT security challenges and ISP.</li> </ol> <p><b>IT future planned actions</b> <i>(12 - 36 months)</i></p> <ol style="list-style-type: none"> <li>1. Continue Cybersecurity scanning on a yearly basis. 2. Implement ISP. 3. Assign security roles to existing staff and hire any security staff needed to manage an Information Security Program</li> </ol>

## APPENDIX A – RISK TREATMENT ACTION PLANS

#	Risk	Risk Detail	Residual Risk Score	Risk Owner	Current State Mitigating Activities	Future State Mitigating Activities	Management Response
2	Utility Market	Exposure to fluctuations in the market price of utilities.	18.75	Deputy General Manager – Georgetown Utilities	<ol style="list-style-type: none"> <li>1) The City has no physical risk and low financial risk from the power supply market.</li> <li>2) ERCOT, the state run system operator, manages and controls the physical matching of supply to demand statewide, thus eliminating the City's exposure to physical supply risk.</li> <li>3) As a Utility within ERCOT, the City takes delivery of all power from ERCOT at the market rate, thus exposing inherent financial risk.</li> <li>4) The City mitigates the inherent financial risk through hedging demand with offsetting, fixed-price power purchase agreements (PPA's) and hedging transmission congestion charges through congestion revenue rights (CRR's) which are forward contracts on congestion. Additional residual financial risk is further mitigated through the industry standard utility practice of passing the variance through to customers as a power cost adjustment factor (PCA). The City does currently use a form of the PCA pass-through, however it is not the current practice to adjust this on a monthly basis.</li> <li>5) The City has a diversified portfolio of PCA's with both short and long terms. The two principle agreements are a 20 year wind and a 25 year solar contract. Together, these two contracts exceed the City's current needs and will accommodate growth.</li> <li>6) The long duration power agreements at fixed price provide long term rate stability through a long term hedge.</li> <li>7) A utility rate study is in progress, to update the most recent study from 2012</li> <li>8) Quarterly financial updates are presented to the GUS Board and the City Council.</li> </ol>	<ol style="list-style-type: none"> <li>1) Continue to enhance the City's forecasting tools and techniques to increase granularity and improve accuracy.</li> <li>2) Continue development of a strategy to meet future peak demand growth with distributed generation and storage rather than remote central generation to mitigate exposure to transmission congestion.</li> </ol>	<p>The City will continue its efforts to mitigate exposure to the utility market:</p> <ol style="list-style-type: none"> <li>1) Implementing rate study recommendations</li> <li>2) Will grow reserves for contingency and market fluctuations to comply with Fiscal &amp; Budgetary Policy</li> <li>3) Will perform rate study every 3 years</li> <li>4) Providing quarterly reports to GUS board</li> <li>5) and City Council.</li> </ol>



## APPENDIX A – RISK TREATMENT ACTION PLANS

#	Risk	Risk Detail	Residual Risk Score	Risk Owner	Current State Mitigating Activities	Future State Mitigating Activities	Management Response
3	IT Asset Management: Data Classification	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	17.00	IT Director	<ol style="list-style-type: none"> <li>1) The City has identified and catalogued its hardware and software via a tool called Lansweeper. This approach ties into an overall information flow enforcement (NIST SP 800-53 Rev. 4 AC-4) which ensures the confidentiality, integrity, and availability of critical data when defined and enforced</li> <li>2) In addition, the City also maintains a manual list of all inventoried applications/ software</li> <li>3) An information classification policy does not currently exist</li> </ol>	<ol style="list-style-type: none"> <li>1) The City should consider classifying data within the system based on its criticality and / or sensitivity (NIST SP 800-53 Rev. 4 RA-2). Classification of data will also help drive the above-mentioned information flow enforcement and help define the City's security architecture</li> <li>2) We recommend the classification of City data to define an appropriate set of protection levels and communication required for special handling Classifications and associated protective controls (including encryption for data at rest and data leak prevention tools) should take into account department needs for sharing or restricting information and the associated business impacts if such data were compromised. Successful data classification in an organization requires a thorough understanding of where the organization's data assets reside and on what applications/devices they are stored. Handling procedures should include details regarding the secure processing, storage, transmission, declassification, and destruction of data.</li> </ol>	<p>The City is currently taking several steps to classify and protect data:</p> <ol style="list-style-type: none"> <li>1) Implementing IT Catalyst Plan – 5 year Strategic Plan</li> <li>2) Developing documented policies to address various IT areas</li> <li>3) Classification of HR and Finance data during Enterprise Resource Planning project</li> <li>4) Payment Card Industry compliance audit</li> </ol> <p>IT sees value in creating a data classification policy that outlines how the city classifies data for each system.</p> <p><b>IT Immediate actions</b>  <i>(next 12 months)</i>            *Work with new ERP vendor to develop classification framework for financial, asset and employee information.</p> <p>Create a Data Classification policy.</p> <p><b>IT future planned actions</b>  <i>(12 - 36 months)</i></p> <p>Classify data in all systems city wide that IT is responsible for administering.</p>

APPENDIX A – RISK TREATMENT ACTION PLANS

#	Risk	Risk Detail	Residual Risk Score	Risk Owner	Current State Mitigating Activities	Future State Mitigating Activities	Management Response
4	IT Access Management	Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	17.00	IT Director	<p>1) New employees and vendors are required to sign off on the Acceptable Use policy</p> <p>2) For financial system, Application Administrator is assigned responsibility of setting permissions for add/removal of users after approval from system owners</p> <p>3) Security administration duties are assigned to various applications whereby all analysts have a designated system/application they are assigned to. Department directors are considered system owners; the IT department facilitates requests/approval of application owner for security access. All IT employees are CJIS certified</p> <p>4) Application vendors must be CJIS certified and CJIS certification is also required in vendor agreements. It was noted that not all applications have a formal process of provisioning and de-provisioning</p> <p>5) Every building is on its own VLAN and segregated, DMZs also exist which is separated by firewalls (in and out). SCADA systems are also air gapped and do not interact with other parts of the network</p>	<p>1) A role-based access scheme should be established to ensure consistent application of user access rights within the system. Users should be assigned their base set of access authorizations based on the concept of “Least Privilege Necessary” to perform their role or job function (as defined within their formal job description). Additional access beyond the previously established role-based access scheme should be formally requested, reviewed for conflicts and approved (NIST SP 800-53 Rev. 4 AC-2). Moreover, Management should consider integrating access rights with data classification efforts identified in Appendix B of this report</p> <p>2) Ensure a process is in place to approve special access requests and timely de-provision access upon notification from HR</p>	<p>The City agrees with these recommendations and is taking the following steps:</p> <p>1) Implementing IT Catalyst Plan – 5 year Strategic Plan</p> <p>2) Implementing 2 factor authentication</p> <p>3) Implementing consistent role based access to CIS and ERP system functions through ERP conversion project</p> <p>IT agrees that additional process and policy is needed to enhance IT access control.</p> <p>IT feels ownership of physical security audits need to be conducted by the department(s) that maintain keys to buildings or the system controlling automated keycard access.</p> <p><b>IT Immediate actions</b></p> <p><i>(next 12 months)</i></p> <p>Implementation of Enterprise Application Access Control policy. Leverage new Systems Admin Lead to identify additional costs and resources to implement auditing of these changes in the future.</p> <p><b>IT future planned actions</b></p> <p><i>(12 - 36 months)</i></p> <p>Identify a way to audit Application Access on a yearly bases. Implement yearly audits for Application Access.</p>

## APPENDIX A – RISK TREATMENT ACTION PLANS

#	Risk	Risk Detail	Residual Risk Score	Risk Owner	Current State Mitigating Activities	Future State Mitigating Activities	Management Response
5	IT Contingency Plan	Loss or inability to continue business due to natural disaster, system capacity or performance issues, interruption in communication, loss or corruption of data, or loss of critical vendors or staff members.	17.00	IT Director	<ol style="list-style-type: none"> <li>1) The City has an extensive data backup strategy is in place in order to ensure that critical data for operations are available in the event of an interruption or incident</li> <li>2) The current data backup plan has redundancy built into the datacenter environmental controls</li> <li>3) Recovery processes are in place to restore systems/assets affected by cybersecurity events. However, CoG is yet to formalize a BCP/DRP</li> <li>4) The City has prepared a five year IT Strategic Plan which includes a plan for implementing business continuity practices over the next 2-3 years</li> </ol>	<p>Plante Moran recommends the City conduct and formalize:</p> <ol style="list-style-type: none"> <li>(1) A Business Impact Analysis (BIA) which identifies and analyzes mission-critical business functions, and then quantifies the impact a loss of those functions would have on the City, and</li> <li>(2) An information system contingency plan to mitigate the risk of critical system and service unavailability. The contingency planning process should occur after a formal Business Impact Analysis (BIA) is conducted, in order to correlate the system with the critical processes and services provided, and based on that information, characterize the consequences of a disruption. Three steps are typically involved in accomplishing the BIA: <ul style="list-style-type: none"> <li>• Determine mission/business processes and recovery criticality</li> <li>• Identify resource requirements</li> <li>• Identify recovery priorities for system resources</li> </ul> </li> </ol>	<p>The City will continue with the efforts already planned to mitigate this risk:</p> <ol style="list-style-type: none"> <li>1) Planning and funding fail-over data center</li> <li>2) Developing and testing protocol to fail-over data center</li> </ol> <p>IT feels this risk is related to the lack of a City Wide Business Continuity plan.</p> <p>IT fully takes responsibility for Disaster Recovery of IT systems, a city wide BCP is needed to identify the Business Impact Analysis and criticality of City wide services to assist with proper implementation of Disaster Recovery activities</p> <p><b>IT Immediate actions</b> <i>(next 12 months)</i></p> <p>Identify how the city wants to address business continuity city wide. Work with Emergency Management to look for third party support to develop a BCP.</p> <p>Leverage new Lead System Admin to start planning and identified resources needed to create a DR plan.</p> <p><b>IT future planned actions</b> <i>(12 - 36 months)</i></p> <p>Develop consistent DR plan that can co-exist with city BCP.</p>

## APPENDIX A – RISK TREATMENT ACTION PLANS

#	Risk	Risk Detail	Residual Risk Score	Risk Owner	Current State Mitigating Activities	Future State Mitigating Activities	Management Response
6	Legislation	Governmental laws change that impact the organization by financial, operating, strategic or compliance issues.	16.36	City Manager's Office	<ol style="list-style-type: none"> <li>1) The City Attorney's office monitors legislative sessions for the City as a whole, and communicates the effects of legislation to appropriate departments</li> <li>2) The Electric Department utilizes a third party engineering firm to monitor potential legislation that could impact the Department</li> <li>3) The City has an agreement with an outside government affairs and advisory firm which specializes in advising and assisting municipalities in legislative activities</li> <li>4) The Transportation Department has developed a detail plan of response to the effects of the City passing the 50,000 population threshold, specifically related to the traffic signal operation. After the 2020 census, the City will be responsible for operating all traffic signals in the City, which is double the number the City currently operates. A large financial commitment will be required to operate and maintain all traffic signals in the City</li> </ol>	<ol style="list-style-type: none"> <li>1) Council and Management should review and closely monitor the status of annexation plans for the City. After the 2020 census, the City will be limited in its ability to perform annexations due to Williamson County's population surpassing 500,000 citizens</li> <li>2) The City should work with legislators to clarify the impact of harmful legislation including revenue caps and limits on debt financing for infrastructure during the City's period of high growth and should stress the removal of local control restrictions that impact citizens ability to impart changes in their local community</li> </ol>	<p>The City will continue its efforts to monitor state actions and advocate for what is best for the organization and community:</p> <ol style="list-style-type: none"> <li>1) Implement Council strategies and tactics related to influence with State government</li> <li>2) Continue supporting TML efforts</li> <li>3) Continue working with government affairs and advisory firm</li> <li>4) Continue to build relationships with other governmental agencies</li> </ol>



## APPENDIX A – RISK TREATMENT ACTION PLANS

#	Risk	Risk Detail	Residual Risk Score	Risk Owner	Current State Mitigating Activities	Future State Mitigating Activities	Management Response
7	Segregation of Duties	The Organization fails to adequately segregate roles and tasks between team members.	16.43	Finance Director	<ol style="list-style-type: none"> <li>1) Each department communicates a personnel change to HR and IT to add/remove/change a staff member's access</li> <li>2) HR and payroll have segregated rolls for processing employee payroll and benefit information. Only Finance has access to process changes within the payroll module</li> <li>3) Segregation within the finance department is maintained by separate individuals processing payroll and accounts payable</li> <li>4) Utilities customer cash receipts are handled through Customer Care front facing staff. Cash drawers are reconciled and closed on a daily basis. Bank deposits are prepared by Customer Care back office operations daily and are couriered to the bank by Police Officers. Revenue financial reporting is done by Finance</li> <li>5) A police officer travels to the cash locations to provide secure courier service on all bank deposits</li> </ol>	<ol style="list-style-type: none"> <li>1) An annual review of user access for all staff members within the City across all programs managed by IT should be performed</li> <li>2) Departments that have not had an internal control review within the past five years should evaluate the design and effectiveness of their internal controls</li> </ol>	<ol style="list-style-type: none"> <li>1) Implementing new CIS and ERP systems which requires thorough review of system segregation controls.</li> <li>2) Cameras being evaluated for various cash areas</li> <li>3) Emphasize and explain segregation of duties attributes during training for new or revised financial policies and procedures.</li> <li>4) Parks &amp; Recreation has segregated deposit duties separate from cashiers.</li> <li>5) Finance is reviewing the segregation of the vendor database duties for the new ERP system.</li> </ol> <p>IT feels this risk requires joint ownership with other departments.</p> <p>IT already has controls in place for user access to computer resources and access to applications.</p> <p><b>IT Immediate actions</b> (next 12 months)</p> <p>Implementation of Enterprise Application Access Control policy. Train IT employees on the new policy. Enforce the new policy on new Enterprise systems as they roll out.</p> <p>Leverage new Lead Admin to identify resources, and costs associated with reviewing user access for all city computer resources and applications.</p> <p><b>IT future planned actions</b> (12 - 36 months)</p> <p>Implement annual reviews/audits of user accounts with access to computers and enterprise applications.</p>
8	Access to Talent	Organization lacks sufficient staffing levels to carry out its routine operations.	11.75	HR Director	<ol style="list-style-type: none"> <li>1) The growth of the City has resulted in a large talent pool for many positions within the City, with some job openings attracting over 300 applicants. Overall, the City gets sufficient applicants for general open positions</li> <li>2) The City is in the process of performing an assessment of retirement eligibility for key personnel</li> <li>3) Departments within the City utilize third party contractors to fill non-key positions on a temporary basis</li> </ol>	<ol style="list-style-type: none"> <li>1) The City should evaluate positions with required specialized certifications and determine whether entry level staff members can obtain certifications after hire</li> <li>2) For specialized positions, including, but not limited to, building inspectors, paving foremen, and traffic engineers, the City should conduct an assessment of staffing levels with a 3-year outlook</li> <li>3) The Fire Department should develop a plan to acquire the necessary EMS personnel talent</li> </ol>	<ol style="list-style-type: none"> <li>1) HR and Fire are continuously developing a recruitment strategy for future station staffing</li> <li>2) The City currently recruits many positions such as 911 dispatcher and Electric Linemen Apprentices in the manner described in mitigating recommendation #1 and continues to review options as new vacancies arise.</li> <li>3) The City works continuously to keep pay and benefits market competitive and HR staff is currently working on enhanced recruitment branding techniques to continue to bring in excellent talent.</li> </ol>

APPENDIX A – RISK TREATMENT ACTION PLANS

#	Risk	Risk Detail	Residual Risk Score	Risk Owner	Current State Mitigating Activities	Future State Mitigating Activities	Management Response
9	Emergency Notification System Failure (ENSF)	The City's Emergency Notification System fails to alert citizens in the event of an emergency.	13.81	Emergency Management Coordinator	<div>1) There is a city-wide emergency notification system consisting of tornado sirens and reverse 911 (Code Red) which are tested on a regular basis. The outdoor warning system is place to notify citizens to take shelter and is not intended to be heard in doors</div> <div>2) The City recently added a position dedicated to Emergency Planning</div> <div>3) Incident Action Plans are developed for large scale community events, such as the Red Poppy Festival</div>	<div>1) The City should communicate Incident Action Plans for large scale events to all parties involved with the event, including the Convention and Visitors Bureau (CVB)</div> <div>2) Management should inform all departments of the operating procedures related to the ENSF</div> <div>3) The EMC should develop basic and advanced emergency management training for key stakeholders in the City (Division Managers) and conduct table top and/or practical training exercises that replicate local level emergencies</div>	The City agrees with these mitigating activities and will prioritize them in the EMC's work plan

## APPENDIX A – RISK TREATMENT ACTION PLANS

#	Risk	Risk Detail	Residual Risk Score	Risk Owner	Current State Mitigating Activities	Future State Mitigating Activities	Management Response
10	Fraud	Customer, third party, or internal fraud occurs resulting in a significant misappropriation of assets and/ or incorrect financial reporting, or corruption/ kickback schemes.	13.75	Controller	<ol style="list-style-type: none"> <li>1) The Finance Department performs a review of a small number of P-Cards to verify the legitimacy of the purchases</li> <li>2) Fixed assets over \$5,000 in value are tracked in the ERP fixed asset module</li> <li>3) Currently no fraud prevention program is communicated to all employees with training to identify and prevent fraud.</li> <li>4) The Finance team indicated internal controls can be strengthened around: <ul style="list-style-type: none"> <li>• Communication, billing and collection from - Planning and Housing and GUS Engineering on construction/ development contracts with developers and as they have limited visibility on project status, progress, completion and timelines of payment due dates. Cannot get My Permit Now to reconcile to Accounting</li> <li>• Processing and internal controls around Grant Administration regarding collections and subsequent compliance reporting</li> <li>• Credit Card (P-Cards) payment procedures are inconsistently applied across City operations</li> </ul> </li> <li>5) The City lacks internal monitoring controls and audit logs around Master File Maintenance on IT databases (employee, customer, vendor, etc.)</li> <li>6) Segregation of duties reduces the chance of fraud</li> <li>7) The City has a personnel policy related to fraud</li> <li>8) A fraud hotline is advertised to the City staff, so that staff can report fraud anonymously. The reports are collected by an outside firm, who sends information to representatives in Human Resources, Finance, and the CMO for investigation. The CMO follows up on any investigations</li> <li>9) Purchasing cards have strict limits to ensure the risk of misuse by a single employee is limited to an average of \$1,000.</li> </ol>	<ol style="list-style-type: none"> <li>1) The Finance Department should perform more robust reviews of P-Card purchases and consider utilizing software to perform regular audits of P-Cards</li> <li>2) The Finance Department should perform annual reviews of P-Card users to evaluate whether the all users actually need P-Cards</li> <li>3) The City should implement a more extensive asset tracking program, utilizing fixed asset tags on assets valued over \$1,000 with consideration of periodic asset audits</li> <li>4) Vendor Ship-To addresses should be limited to a “drop down” list consisting only of City facilities</li> <li>5) The City should consider developing a fraud awareness and prevention training program with active participants across all City departments</li> <li>6) All changes to IT databases deemed to be material should be tracked on an Audit File Log and reviewed by someone without access to the databases</li> </ol>	<ol style="list-style-type: none"> <li>1) Asset tracking and vendor shipping will improve as part of the ERP project.</li> <li>2) The City has already implemented and conducted training on grant tracking and reporting.</li> <li>3) Staff are currently developing a citywide fraud awareness and reporting training.</li> </ol>

## APPENDIX A – RISK TREATMENT ACTION PLANS

#	Risk	Risk Detail	Residual Risk Score	Risk Owner	Current State Mitigating Activities	Future State Mitigating Activities	Management Response
II	Health & Safety	Exposure to potentially significant workers' liabilities due to the inability to maintain compliance with applicable health and safety laws and regulations.	13.04	HR Director	<ol style="list-style-type: none"> <li>1) All Public Works and Utility departments have a robust safety program consisting of monthly safety training, daily safety summaries, semi-monthly safety meetings, and detailed safety policies. Public Works departments also provide sufficient safety equipment to all relevant staff members</li> <li>2) The Fire and Police Departments have a robust line of safety gear, training, fitness assessments, inspections, and safety policies</li> <li>3) All safety incidents are communicated to Human Resources for review and to work as a liaison between the department and the employee</li> <li>4) The Airport requires all non-airport employees to be escorted by a staff member with knowledge of Air Traffic Control communication</li> <li>5) Parks and Recreation requires safety maintenance with swimming pools to ensure chemicals are in balance</li> </ol>	<p>Overall, the City has robust health and safety procedures and should consider adding the following:</p> <ol style="list-style-type: none"> <li>1) The Library should develop clear policies and procedures on a course of action when a customer, employee, or volunteer is injured at the facility.</li> <li>2) The City should review the lifeguard policy for pool facility rentals. The City currently does not provide a lifeguard for pool rentals by the Georgetown Independent School District and does not require GISD to provide their own lifeguard.</li> <li>3) Consider adding an Active Shooter response plan</li> </ol>	<ol style="list-style-type: none"> <li>1) HR and Library will work together to develop consistent injury procedure</li> <li>2) The City has met with GISD swim coaches to brainstorm ways to mitigate lifeguard risk and is drafting a facility use agreement that outlines the lifeguard requirements of the City and GISD</li> <li>3) HR and Police are developing Active Shooter training for departments</li> </ol>

## APPENDIX A – RISK TREATMENT ACTION PLANS

#	Risk	Risk Detail	Residual Risk Score	Risk Owner	Current State Mitigating Activities	Future State Mitigating Activities	Management Response
12	IT Incident Response Management	Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	12.00	IT Director	<ol style="list-style-type: none"> <li>1) The City has no formalized or documented information security incident response procedure</li> <li>2) CoG's IT department has an informal (undocumented/ad-hoc) resolution process to ensure appropriate steps are taken to respond to incidents. The process is triggered in the event of a report/discovery of compromise, loss, or theft of system data</li> </ol>	<p>We recommend the City implement a formal incident response plan including:</p> <ol style="list-style-type: none"> <li>1) Provide a roadmap for implementing its incident response capability;</li> <li>2) Describes the structure and organization of City of Georgetown's incident response capability;</li> <li>3) Provides a high-level approach for how the incident response capability fits into City of Georgetown as a whole and the overall Family of Companies;</li> <li>4) Meets the unique requirements of City of Georgetown's mission, size, structure, and functions;</li> <li>5) Defines reportable incidents as well as requirements and guidelines for external communications and information sharing (e.g., what can be shared with whom, when, and over what channel);</li> <li>6) Provides metrics for measuring the incident response capability within the organization;</li> <li>7) Defines the resources and management support needed to effectively maintain and mature an incident response capability; and</li> <li>8) Is reviewed and approved by senior management</li> </ol>	<p>IT agrees a formal process and procedures need to exist to manage cybersecurity incidents appropriately.</p> <p><b>IT Immediate actions</b> <i>(next 12 months)</i></p> <p>Implement Incident response policy. Train IT staff on procedures to ensure policy is being met.</p> <p><b>IT future planned actions</b> <i>(12 - 36 months)</i></p> <p>Document formal incident response plan including all recommendations by Plante.</p>
13	Utility Outage	The City is unable to respond to mass failures of electrical, water, or sewage outages in a timely manner.	11.89	Utility Director	<ol style="list-style-type: none"> <li>1) Control Center has monitoring alarms in the event of outages</li> <li>2) Control Center has an outage management system to diagnose location of fault and provide area of impact and customer count</li> <li>3) Response plan is in place for water, wastewater, and electric system failures.</li> <li>4) Regular maintenance tracking of all critical equipment; replacement is made when showing signs of degrading through testing</li> </ol>	<ol style="list-style-type: none"> <li>1) Maintain equipment useful lives schedule and proactively monitor components which have reached their useful lives</li> <li>2) Perform a vulnerability assessment to judge your preparedness for handling the increased likelihood for power outages</li> </ol>	<p>Emergency Response Procedures have been expanded to include establishment of an Operations Command Center procedure for emergency response for large scale utility outages that do not rise to the level of EOC activation.</p>

## APPENDIX A – RISK TREATMENT ACTION PLANS

#	Risk	Risk Detail	Residual Risk Score	Risk Owner	Current State Mitigating Activities	Future State Mitigating Activities	Management Response
14	Disaster Recovery / Business Continuity Planning	Inability of the organization to continue key business processes during a potential disaster due to lack of sufficient disaster recovery planning and/or execution.	11.60	City Manager's Office	<ol style="list-style-type: none"> <li>1) Most city staff members are able to work remotely via Virtual Desktop Infrastructure (VDI)</li> <li>2) The Public Works Departments conduct assessments of potentially hazardous situations (ex: tree trimming to prevent outages during windstorms)</li> <li>3) The Fire and Police Departments can immediately route 911 calls to the Williamson County 911 center</li> <li>4) Tabletop disaster recovery simulations are performed on an annual basis by the Emergency Management Coordinator in conjunction with the Fire Department</li> <li>5) No backup plan in place at Airport if fueling system or lighting vault fails. This has been identified as a weakness and accounted for in the Airport Master Plan to remediate over the next 5 years.</li> <li>6) No DR/BCP plan at the Library, Communications, Convention &amp; Visitor's Bureau, Customer Care and Inspection Services</li> <li>7) Back in 2005, the Municipal Court had a system crash and were unable to recover records. They had to recreate 2.5 months of records and it took about 6 months. The issue has not been resolved</li> </ol>	<ol style="list-style-type: none"> <li>1) The City has inconsistent DR/BCP across the organization. Some departments have a robust plan and others have none. A DR/BCP should be developed for every City department. Each of these department-level plans should then be integrated into a city-wide plan</li> <li>2) Tabletop disaster recovery simulations should be performed with all City Departments</li> </ol>	<ol style="list-style-type: none"> <li>1) As the City buys new or upgrades existing software, we are prioritizing cloud options that improve security and access</li> </ol>

## APPENDIX A – RISK TREATMENT ACTION PLANS

#	Risk	Risk Detail	Residual Risk Score	Risk Owner	Current State Mitigating Activities	Future State Mitigating Activities	Management Response
15	Billing for Citizen Services	Citizens are billed incorrect amounts or not billed at all for citizen services.	11.37	Customer Care Director	<ol style="list-style-type: none"> <li>1) Rates and/or fees for Utility Services, Building Inspection Services, Animal Services, Permits, Fire, Police and Airport are approved by Council</li> <li>2) Parks and Recreation rates are set and approved by the Parks and Recreation Director and submitted to the Council annually</li> <li>3) Customer Care utilizes systems built into the meter data management (MDM) and customer information systems (CIS) that apply validation methodology to detect abnormal consumption or amount billed. These “exceptions” are identified in the systems for staff to review and validate manually (referred to as “Edit Process”)</li> <li>4) Billing for EMS services is performed by a 3rd party service and any hardship write downs require the Fire Chief’s approval</li> <li>5) Departments handling cash perform daily cash reconciliations</li> <li>6) The Municipal Court clerks review all tickets/citations before being sent to the recipient</li> <li>7) The Code Enforcement Department maintains evidence of violations to be billed, and the Energy Services Department maintains the police report as evidence for billing for damages</li> <li>8) Airport uses a third party appraisal for lease amounts along with fuel prices set by City Council</li> </ol>	<ol style="list-style-type: none"> <li>a. The fine schedule for the Municipal Court citations should be restricted to specific users</li> <li>b. All invoices should be created in a single system across the City and remit-to addresses should be limited by a “drop-down” function consisting of only addresses the City accepts payments</li> <li>c. Management should consider a third party revenue recognition study to validate all sources of revenue are complete and accurate across the City operations</li> <li>d. An outside party, Emergicon, reviews billing for EMS incidents as there are various rates depending on citizen’s ability to pay. Emergicon also collects funds and this helps reduce the occurrence of billing errors and improves collections. However, Emergicon also writes off funds and there is no reconciliation of EMS revenue to billings. We recommend the City enhance reconciliation controls around billing procedures and perform internal audits of quality control and verification of vendor compliance.</li> </ol>	<ol style="list-style-type: none"> <li>1) Implementing a new ERP system will include a thorough review of the Accounts Receivable/Billing module.</li> <li>2) Once Emergicon has completed a full fiscal year of billings and collections, the City can audit and evaluate the performance and compliance of Emergicon’s processes and procedures.</li> </ol>

## APPENDIX A – RISK TREATMENT ACTION PLANS

#	Risk	Risk Detail	Residual Risk Score	Risk Owner	Current State Mitigating Activities	Future State Mitigating Activities	Management Response
16	Composition of Tax Base	Changes in the balance of commercial and residential tax base result in losses of revenue from taxes.	10.63	City Manager's Office	<ol style="list-style-type: none"> <li>1) The City has performed a detailed mapping of how each square mile of the city will be used in the future</li> <li>2) The City Manager's Office completes regular fiscal impact models to determine the effects of commercial vs. residential development</li> <li>3) The Economic Development Department has established a comprehensive strategic plan</li> <li>4) Economic Development relies on demographic research for talking to prospects regarding future development. Works closely with the Planning Department</li> <li>5) The Fire Department should be involved in all communications regarding commercial development in order to ensure the Department is able to acquire the necessary equipment to manage emergencies at large scale commercial properties</li> <li>6) The Fire Department has increased its staff to respond to an increase in calls for service. The rate of EMS calls for service is growing at double the rate of population</li> <li>7) The City is updating its Comprehensive Plan which will include an update to the future land use plan</li> <li>8) Planning Dept. promotes and encourages a varied level of housing products and commercial tax base per the Comprehensive Plan.</li> </ol>	<ol style="list-style-type: none"> <li>1) The City should communicate potential new commercial and residential development to directly impacted City departments and evaluate how new development would affect each directly impacted department</li> <li>2) Management should utilize a concentration strategy that is flexible and supported by realistic expectations</li> </ol>	<p>The City is updating its Comprehensive Plan through a robust citizen engagement process during 2018/19. This plan will identify community standards and goals for growth.</p> <p>City staff from various departments impacted by development meet with the City Manager's Office on a bi-weekly basis to discuss major development applications as well as to collaborate and problem solve on various issues.</p>
17	Grant Obligations	Organization fails to meet grant covenant requirements.	10.55	Controller	<ol style="list-style-type: none"> <li>1) Grants filings across the City are monitored by various personnel within the Finance Department</li> <li>2) Grant applications require City Council approval per the City's Fiscal and Budgetary Policy</li> <li>3) Federal and State grants require compliance filings and, if omitted, could impact future grant funding, as well as result in audit findings</li> </ol>	<ol style="list-style-type: none"> <li>1) The City should designate a staff member as a Grant Administrator. This staff member should be responsible for maintaining a repository of all grants being applied for, awarded, contact person, and any required filings associated with each grant. City should require that all Grants be managed through the new Grant Administrator</li> <li>2) A Grant Status Report should be provided on a periodic basis to the City Manager's office for potential budget considerations</li> </ol>	<p>The City has completed these recommendations. The Controller is the Grant Administrator. A new policy was implemented in the spring and the status report is presented to Council in the quarterly financial report.</p>



APPENDIX A – RISK TREATMENT ACTION PLANS

#	Risk	Risk Detail	Residual Risk Score	Risk Owner	Current State Mitigating Activities	Future State Mitigating Activities	Management Response
18	IT Third Party Roles & Responsibilities	Security roles and responsibilities are not established for all third-party service providers and lack clear contractual obligations for service level agreements and KPI's.	10.00	IT Director	<div>1) The City has identified trusted partners with respect to hardware and hosted applications</div> <div>2) Roles and responsibilities have been established but are not formally documented. Within the workforce, absence of a formal documentation poses a risk for segregation of duties and with third parties, accountability may be lacking</div> <div>3) The contract between City of Georgetown and the service provider does not specifically outline the roles and responsibilities related to Cybersecurity controls handled by each organization</div> <div>4) There is no monitoring of external party use of the system for potential Cybersecurity events</div>	<div>We recommend management take the following actions:</div> <div>1) Clearly identify the cybersecurity responsibilities to be outlined in the contract with the service provider including roles for identification, response, and recovery procedures</div> <div>2) Establish Key performance indicators for third-party responsibilities including number of events, data breaches, number of notifications</div> <div>3) Continuously monitor contract SLA's and established key performance indicators</div>	<div>IT has been working to ensure new contracts meet a higher level of security requirements. For example the Office 365 contract with Microsoft has advanced alerting for things like elevation in access privileges and enhanced reporting to view our security posture at any time.</div> <div>IT manages KPI's for 3<sup>rd</sup> party contracts through simple notification of security events that can follow the city's Information Security Response plan should provide adequate documentation for security events.</div> <div>Incident response risks are being addressed under Risk # 3 on this document.</div> <div><b>IT Immediate actions</b></div> <div><i>(next 12 months)</i></div> <div>Continue to monitor all new contracts to ensure proper cybersecurity language exists.</div> <div>Require all vendors to use multi factor authentication to access city resources.</div> <div><b>IT future planned actions</b></div> <div><i>(12 - 36 months)</i></div> <div>Review older contracts and make notes of where changes are needed during contract renewals.</div>

APPENDIX A – RISK TREATMENT ACTION PLANS

#	Risk	Risk Detail	Residual Risk Score	Risk Owner	Current State Mitigating Activities	Future State Mitigating Activities	Management Response
19	Vendor Reliance	Any termination of, or adverse change in, the Organization's relationships with its key suppliers, or loss of the supplies in support of one of the organization's key services.	9.81	Purchasing Manager	<div>1) The majority of City Departments have multiple vendors available to supply goods &amp; services and would not face disruption if they had to switch vendors</div> <div>2) We noted 3 departments that have a reliance on key vendors and they are closely monitoring this process: Transportation (asphalt and concrete), Fire Department (specialty vehicle repair) and Animal Services (specialty veterinarian drugs and feed)</div>	<div>1) Assign one person the responsibility of monitoring all key vendors to the City</div> <div>2) Create a subsidiary listing of all key vendors with contract details, SLA's and performance metrics</div> <div>3) Report back to City Manager when it is determined a vendor may become insolvent or is not meeting SLA's</div> <div>4) Prior to contract renewal, negotiate with all key vendors to capture volume discounts and preferred pricing</div> <div>5) Management indicated Garland Power &amp; Light currently reconciles their meter data to the scheduling data and the transaction settlement engine. This could be done in house but would require additional headcount as the process runs 24/7. Management should consider a cost/benefit study to do this in-house</div>	<div>The new ERP will enhance the ability to analyze vendor and contract details.</div> <div>The City's purchasing policy receives quotes and/or formal bids for purchased over \$3,000. Purchases over \$50,000 are approved by Council so more review is given to these large expenditures.</div> <div>The management acknowledges that certain items noted are "sole source" which provides a reliance on key vendors in limited situations/purchases.</div>

APPENDIX A – RISK TREATMENT ACTION PLANS

#	Risk	Risk Detail	Residual Risk Score	Risk Owner	Current State Mitigating Activities	Future State Mitigating Activities	Management Response
20	IT Critical Security Event Identification	A formal risk event identification process is not in place to identify, classify and resolve security events	9.00	IT Director	<div>1) Currently there are a variety of log generation methods in place for the system, however there is no catalog of security event types being identified and reviewed within the logs by security professionals</div> <div>2) As noted in the Segregation of Duties risk, there are no documented audit log reviews of changes made to critical City databases</div>	<div>1) Identify high risk events that can be alerted from current logging capabilities (NIST SP 800-53 Rev. 4 AU-6). Potential high risk events can be discerned through the risk assessment process (NIST SP 800-53 Rev. 4 RA-3), penetration testing, and best practice documentation. Some common threat events include:<ul style="list-style-type: none"><li>Multiple failed login attempts</li><li>Elevations in access privileges</li><li>Changes to application code</li><li>Changes to security settings</li><li>Process specific actions</li></ul></div> <div>2) Consider alert generation techniques for risky events such as devices that connect to the network without authorization</div> <div>3) Identified events should be responded to in accordance with the organization’s Incident Response Plan</div>	<div>IT does not currently have designated security staff. This makes it challenging to implement controls at this level because of the time and knowledge necessary to keep a proactive approach maintained. IT agrees we should have an advanced alerting process on high risk events however continuing to maintain these types of processes can be staff intensive.</div> <div><b>IT Immediate actions</b> <i>(next 12 months)</i> Hire a Lead System Administrator (approved for FY19) to assist with security activities.</div> <div>Identify high risk events that occur in current logging tools. Research methods for alerting based on events. Research staff time needed to implement and maintain an alerting process that always follows best practices. Research managed security services and costs. Discuss options with City Manager’s Office for implementation.</div> <div><b>IT future planned actions</b> <i>(12 - 36 months)</i> Create an alerting strategy/process that alerts staff when appropriate. Implement alerting for high risk events.  Implement managed security services if feasible.</div>

## APPENDIX A – RISK TREATMENT ACTION PLANS

#	Risk	Risk Detail	Residual Risk Score	Risk Owner	Current State Mitigating Activities	Future State Mitigating Activities	Management Response
21	IT Security Awareness, Training and Education	Personnel are not informed of potential IT threats to the organization and are unable to respond effectively.	9.00	IT Director	<ol style="list-style-type: none"> <li>1) The City has implemented an Acceptable Use Policy amongst other policies around proper use of computers and accessing digital information. However, to ensure compliance, there is a need to assess employee's understanding of policies and response to cybersecurity threats via periodic awareness and training</li> <li>2) IT staff monitors and reports email scams to all employees in an effort to increase awareness</li> </ol>	<ol style="list-style-type: none"> <li>1) Rely on end users as the first line of defense to limit exposure to social engineering frauds and threats</li> <li>2) Consider increasing complexity of password requirements</li> <li>3) Create a formal IT Awareness training and provide to all employees on a periodic basis</li> <li>4) Require employees to formally acknowledge in writing that they have read and understand the security awareness training, and that they recognize the ramifications of non-compliance</li> </ol>	<p><b>IT Immediate actions</b> <i>(next 12 months)</i></p> <p>Implement city wide security awareness program and training. Partner with HR to leverage use of LMS for security training.</p> <p><b>IT future planned actions</b> <i>(12 - 36 months)</i></p> <p>Continue to provide security awareness training and review annually for new material and best practices.</p>
22	Fire Department Failure	The Fire Department is not adequately equipped to handle responses to emergencies in the City.	8.00	Fire Chief	<ol style="list-style-type: none"> <li>1) The GFD studies data points to best position their resources in order to minimize response times. In instances when there are no resources available, GFD has agreements with third party ambulance providers who are obligated to provide the same response time as the GFD</li> <li>2) Also, the GFD have mutual aid agreements with neighboring communities to assist in calls when the City is not available</li> <li>3) The GFD indicated they perform fire inspections of public buildings (schools, hospitals, government buildings, etc.) but there are not enough resources to do fire inspections/ capacity evaluations on all businesses in the City</li> <li>4) The City is currently building two stations to ensure adequate response to the growing population</li> </ol>	<ol style="list-style-type: none"> <li>1) Consider an independent third party evaluation study of the GFD capabilities, response metrics and resource allocations to evaluate if there needs to be changes to the current resource allocation model</li> <li>2) Consider cooperative agreements with ESD8 and/or contiguous municipalities to elevate synergistic programs (co-located/co-operated) fire stations and boundary drops (enhanced auto-aid).</li> <li>3) Consider making licensed buildings be required to be inspected annually. Also, consider a self-inspection program for low risk properties and/or an inspection matrix as follows: <ul style="list-style-type: none"> <li>• Low Risk – every 3 years</li> <li>• Medium Risk – every 2 years</li> <li>• High Risk – annually</li> </ul> </li> <li>4) Management should consider the implications for property owners and businesses when the Public Protection Classification (PPC) issued by the Insurance Services Organization (ISO) is not performed, as there may be a negative impact if not inspected annually.</li> </ol>	<p>GFD regularly reviews KPIs and communicates with city management on service delivery standards. Mutual aid agreements are in place for assistance when additional resources are needed. Additionally, GFD is exploring partnership opportunities on a long-term future station with Round Rock.</p> <p>A Fire inspector has been added to the staff for FY19 to help address the backlog of inspections and keep up with the growing number of business inspections.</p>

## APPENDIX A – RISK TREATMENT ACTION PLANS

#	Risk	Risk Detail	Residual Risk Score	Risk Owner	Current State Mitigating Activities	Future State Mitigating Activities	Management Response
23	Physical Security	Facilities are not appropriately secured from unauthorized access.	9.00	Asst. Parks & Recreation Director	<p>Overall the City has robust physical securities controls in Place:</p> <ol style="list-style-type: none"> <li>1) Customer Care and Municipal Courts have robust physical security programs in place. Safes are utilized for cash and cameras cover registers and safes. Dual access controls with keys and codes are used at cash access points</li> <li>2) Most City buildings require access badge/ fob to enter restricted (non-public) areas.</li> <li>3) Police, Fire and Energy Services departments have restricted access areas</li> <li>4) However, we noted several areas with limited physical security controls: <ul style="list-style-type: none"> <li>• Animal Services – lack of physical security is a major issue as animals have been stolen. Cash is not well controlled and cameras are not in place on critical areas. The safe is not adequately secured.</li> <li>• Building Inspection Services, Public Works, GIS, Systems Engineering and the Georgetown Municipal Complex have poor physical security</li> </ul> </li> </ol>	<ol style="list-style-type: none"> <li>1) Consider taking inventory of all key cards to validate none have been stolen or lost</li> <li>2) Consider development of physical security training for all personnel regarding safeguarding of assets, restrictive access to high risk areas, etc. The City must support integrity of physical security through the organization with the assistance of the City's Risk Manager</li> <li>3) Standardize a consistent security plan across all locations appropriate for each facility</li> <li>4) The City currently monitors physical access to the facility where IT resides to detect and respond to physical security incidents. However, CoG does not review physical access logs periodically</li> </ol>	<ol style="list-style-type: none"> <li>1) Cameras are being evaluated for various cash areas</li> <li>2) Security access will be part of the current facilities study</li> <li>3) Security access will be evaluated with the opening of each new or renovated facility.</li> </ol>
24	Freedom of Information Act (FOIA)	Non-compliance with FOIA requests	6.22	City Secretary	<ol style="list-style-type: none"> <li>1) The procedure is for all FOIA requests to enter through Legal. They will decipher the request and handoff to the City Secretary office to obtain information.</li> <li>2) FOIA request process is currently being transferred from Legal to City Secretary and is approximately 90% complete</li> <li>3) GovQA is an electronic system used to maintain and track FOIA requests.</li> </ol>	<ol style="list-style-type: none"> <li>1) When the transfer of FOIA request process is complete, consider documenting the process with written policies and procedures</li> <li>2)</li> </ol>	<ol style="list-style-type: none"> <li>1) The City has completed the transfer of FOIA request process to the Open Records Coordinator in the City Secretary's office.</li> <li>2) Citywide training has been completed by the Open Records Coordinator to provide guidelines and consistency to the process.</li> <li>3) The City Secretary Department is in the process of completing Policies and Procedures for FOIA and should have completed within the next month.</li> </ol>

## APPENDIX A – RISK TREATMENT ACTION PLANS

#	Risk	Risk Detail	Residual Risk Score	Risk Owner	Current State Mitigating Activities	Future State Mitigating Activities	Management Response
25	Police Failure	The Police Department is inadequately equipped to respond to emergencies or responds in an unauthorized manner.	6.00	Police Chief	<ol style="list-style-type: none"> <li>1) Police department is aware of people, process, technology and regulatory requirements</li> <li>2) Robust controls are in place to monitor progress and key performance indicators</li> <li>3) A culture of clearly communicating expectations, behaviors, and training is in place so officers are held accountable for their actions</li> <li>3) Guardian Tracking is a day-to-day tracking of personnel performance entry recordkeeping. Police management reviews and a conversation with the employees occurs when they handle situations incorrectly</li> <li>4) Training includes the following: <ul style="list-style-type: none"> <li>• Handling of persons with mental illness</li> <li>• Defusing techniques to encourage peaceful tactics</li> <li>• Non-lethal methods of restraint</li> </ul> </li> <li>5) Internal affairs division investigates all complaints against officers</li> </ol>	<ol style="list-style-type: none"> <li>1) Develop the following Key Risk Indicators (KRI's) and monitoring controls which may indicate a risk event is about to occur <ol style="list-style-type: none"> <li>a. Increase in City crime rates</li> <li>b. Increase in police misconduct/brutality incident claims</li> <li>c. Increase in squad car accidents</li> <li>d. Excessive overtime</li> <li>e. Unexpected cost overruns/continuous unfavorable budget variances</li> <li>f. Increase in dismissed cases due to insufficient evidence, improper procedures or failure to follow legal standards for police</li> </ol> </li> </ol>	<ol style="list-style-type: none"> <li>1) The City will monitor quality of life crimes within the city and identify strategies for reduction where feasible.</li> <li>2) The City will monitor and investigate all complaints, including use of force and pursuits and will identify strategies for reduction where feasible.</li> <li>3) The City will monitor police overtime and identify strategies for reduction where feasible.</li> <li>4) An annual report of crime statistics is presented publically to the City Council.</li> </ol>
26	Talent Management	Organization lacks a clear assessment and evaluation process to align qualified employees with specific business requirements and needs.	5.42	HR Director	<ol style="list-style-type: none"> <li>1) The City personnel policy requires bi-monthly performance discussions with all employees</li> <li>2) Formal annual and mid-year performance evaluations, including employee development and training plans, are performed on all employees</li> <li>3) Energy Department has a robust training curriculum with a 4-year apprentice program</li> <li>4) Police department uses Guardian Tracking to evaluate officer performance daily</li> </ol>	<ol style="list-style-type: none"> <li>1) Have HR department work collaboratively with business lines to gain in depth knowledge of resource needs and constraints</li> <li>2) Consider using an outside party for diversity in pre-hire assessments</li> </ol>	<ol style="list-style-type: none"> <li>1) HR staff is developing a supervisor survey to identify employee development for current and future roles</li> <li>2) HR staff trained all supervisors in 2017 on proper hiring techniques including ways to overcome various forms of hiring bias</li> <li>3) The city conducted an employee survey in 2016 and again in 2018. 79% of employees believe their job makes good use of their skills and abilities. 84% believe their job provides opportunities to do challenging and interesting work.</li> </ol>
27	Records Management	No records management policy is in place, adhered to, or is inadequately designed.	5.27	Records Program Manager	<ol style="list-style-type: none"> <li>1) The City's records retention policy is in line with the Texas State Library records retention policy. The department receives alerts from the state library of any changes to policy</li> <li>2) Finance indicated they are unclear on how electronic records storage should be handled</li> <li>3) Parks and Recreation has a large quantity of waivers and registration hard copy forms</li> <li>4) Animal Services has a lack of electronic records and believes there is a risk of information loss</li> </ol>	<ol style="list-style-type: none"> <li>1) Formalize Records Management policy regarding digital records and communicate to all departments</li> <li>2) Consider additional training on electronic records management</li> <li>3) Consider digitizing Parks &amp; Recreation forms</li> </ol>	<ol style="list-style-type: none"> <li>1) The Records Team is training various departments on retention, destruction of records and digitalization of records.</li> <li>2) Policies and Procedures have been completed and implemented.</li> <li>3) The following information has been made available to employees via the internal GO site: <ol style="list-style-type: none"> <li>a. Records Management Policy &amp; Procedures</li> <li>b. Retention Schedules</li> <li>c. Off-site storage information</li> <li>d. Destruction authorization forms</li> </ol> </li> </ol>

APPENDIX A – RISK TREATMENT ACTION PLANS

#	Risk	Risk Detail	Residual Risk Score	Risk Owner	Current State Mitigating Activities	Future State Mitigating Activities	Management Response
28	Regulatory Filings	Failure to comply with regulatory filings such as GASB, EPA, etc.	5.20	Controller	<div>1) Water Services completes Environmental Protection Agency (EPA) and Texas Commission on Environmental Quality (TCEQ) permit reports every 3-5 years</div> <div>2) Finance prepares annual CAFR and SEFA which is submitted to the clearinghouse</div> <div>3) Customer Care prepares annual filings on storm water use survey breaking out how much water was taken in to the system.</div> <div>4) City of Georgetown has an exemption from complying and filing necessary reports mandated by Senate Bill 898 (reducing energy consumption in City owned facilities) &amp; administered via the State Energy Conservation Offices (SECO) because of the 100% renewable designation.</div> <div>5) Customer Care is required by TCEQ to report water quality testing results to customers on an annual basis. Deadline for customer communications is 7/1. GUS must certify with TCEQ by 5/1 that we provided water quality testing results to water purveyors that obtain wholesale water from GUS.</div> <div>6) Energy Services relies on outsource provider Snyder Engineering for all regulatory findings</div> <div>7) Utility services is subject to an annual requirement with the ERCOT to validate that a risk management plan is in place</div> <div>8) Airport has a significant amount of regulatory filings ranging from EPA, TCEQ, Stormwater, Airplane inventory, and Property Taxes through MCAT. Use Microsoft Outlook as reminders</div> <div>9) Fire Dept. has numerous state health services filings regarding training, certifications, incidents, fatalities, etc.</div>	<div>1) There is a significant amount of regulatory filings across the City. Management should consider a consolidated Regulatory Compliance Landscape (RCL) ledger be compiled to have one list of all requirements outlining the filing dates. Further, Management should store this on a shared drive and assign all filings to an owner who is required to indicate when the filing is complete. Someone should be responsible for checking for missed filings</div>	Management is evaluating a contracts management system to track and comply with contractual and regulatory requirements. This may be part of the ERP implementation or a stand-alone system.

## APPENDIX A – RISK TREATMENT ACTION PLANS

#	Risk	Risk Detail	Residual Risk Score	Risk Owner	Current State Mitigating Activities	Future State Mitigating Activities	Management Response
29	Succession Planning	Leadership talent within the organization is insufficiently developed to provide for orderly succession in the future.	4.39	HR Director	<ol style="list-style-type: none"> <li>1) No formal succession planning in place. Per Human Resources, they emphasize internal cross training to grow future leaders from inside the City organization</li> <li>2) The City is in the process of performing an assessment of retirement eligibility for key personnel</li> </ol>	<ol style="list-style-type: none"> <li>1) The City should consider an outside party to implement a formal Succession Plan</li> <li>2) Consider a mentor shadowing program to protect the City against unplanned terminations or leaves of absences</li> </ol>	<ol style="list-style-type: none"> <li>1) City initiated first Emerging Leader training program in 2018 with 20 graduates. Anticipate annual opportunity to grow employees at various levels each year</li> <li>2) Supervisory Series initiated in 2017 and successfully completed by 168 supervisors. Additional curriculum to be added this year aimed at growing managerial skillset of all city supervisors</li> <li>3) The city conducted an employee survey in 2016 and again in 2018. 76% of employees plan to continue working for Georgetown for 5+ years, which is significantly higher than most employers.</li> </ol>
30	Budget and Planning	Budgets and business plans are not realistic, based on appropriate assumptions, based on cost drivers and performance measures, accepted by key managers, or useful or used as a monitoring tool.	3.24	Finance Director	<ol style="list-style-type: none"> <li>1) The City uses a robust budget and planning tool across the organization using historical data supplemented with forward looking analytics. Each Department head formalizes their budget and forward to Finance for consolidation</li> <li>2) Finance utilizes Excel to manually consolidate the budgets and upload into the ERP system</li> <li>3) Final budgets are presented to City Council for review and approval</li> <li>4) Quarterly budget to actual reports are presented to City Council</li> </ol>	<ol style="list-style-type: none"> <li>1) Certain departments such as utilities, water, electric, etc. count on supplemental data to prepare their budget (see Data Governance risk #27). We recommend management validate and document the completeness and accuracy of assumptions for all budget line items</li> <li>2) Management should set a clearly defined threshold for all material variances to be explained (e.g. +/-XX% and \$YY,YYY)</li> </ol>	<ol style="list-style-type: none"> <li>1) The new ERP system will facilitate a central location of budget development information and reporting</li> <li>2) Finance Administration's performance measures include budget to actual variance targets</li> </ol>
31	Tax	Non-compliance with state or federal tax law.	3.00	Controller	<ol style="list-style-type: none"> <li>1) Finance maintains schedule of tax payments and receipts to/ from County, State and Federal authorities</li> </ol>	<ol style="list-style-type: none"> <li>1) Consider the creation of a master tax filing schedule and reporting to City Manager</li> </ol>	The City agrees with this recommendation.
32	State / Federal Regulations	Failure to comply with new or existing federal or state regulations.	2.44	Controller	<ol style="list-style-type: none"> <li>1) Building Inspection Services provided that maintaining state licenses and Continuing Professional Education (CPE) is a challenge</li> <li>2) State regulations require the Police Department to report all racial profiling and crime data</li> <li>3) Parks and Recreation indicated that there is a State Health and Safety Code that requires public play equipment comply with the American Society for Testing Materials (ASTM) F1487-07 which provides performance standards for public playgrounds and this is NOT being done on a routine basis</li> </ol>	<ol style="list-style-type: none"> <li>1) Develop a Citywide license and CPE tracking system</li> <li>2) Develop a process to ensure all City playgrounds comply with ASTM F1487-07. The code does not require a formal inspections process, just that the City complies with the ASTM F1487-07 standard</li> </ol>	<p>The City will review a tracking system in context of all other technology needs. Employees and supervisors will continue to be responsible for tracking individual and departmental CPE and licensing.</p> <p>Parks Department is working on a schedule to evaluate older parks to replace equipment as needed. Newer parks and equipment is compliant.</p>



APPENDIX A – RISK TREATMENT ACTION PLANS

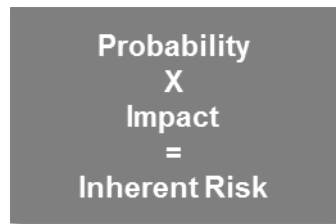
#	Risk	Risk Detail	Residual Risk Score	Risk Owner	Current State Mitigating Activities	Future State Mitigating Activities	Management Response
33	Leadership	The people responsible for the important City processes do not or cannot provide the leadership, vision, and support necessary to help employees be effective and successful in their jobs.	2.42	City Manager	<div>1) All departments we interviewed provided the same issue on leadership – there is a strong management base that sets realistic strategic objectives and has an open communication line with each department head</div> <div>2) Leadership has frequent meetings with department heads to check on status of operations and those concepts are clearly communicated throughout the organization</div> <div>3) Detail performance evaluations are done at all levels of the City government and each employee is evaluated for job performance</div>	<div>1) The City should consider an upward feedback program to validate lower levels of employees are satisfied with management’s performance</div>	<div>1) A 360 evaluation process was implemented last year for Directors and will be rolled out to mid-level management in the upcoming year.</div> <div>2) The city has implemented a bi-monthly check-in program where employees have the capability to provide upward feedback to their supervisor.</div> <div>3) The city conducted an employee survey in 2016 and again in 2018. Employee response rates were 85% and 82% respectively and the city has involved employees in tactical action planning to further improvement engagement and enablement.</div>

# Appendix B

## Information Technology Executive Summary

## APPENDIX B

### CYBERSECURITY RISK ASSESSMENT EXECUTIVE SUMMARY


$$\begin{array}{c} \text{Probability} \\ \times \\ \text{Impact} \\ = \\ \text{Inherent Risk} \end{array}$$

**Inherent Risk:** Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the probability that a threat event will occur and the resulting impact. The probability and impact analysis leads to identification of inherent risk (i.e., risk without consideration of controls) to the IT environment. With this information, organizations can determine the acceptable level of risk for delivery of services and can express this as their risk tolerance.

Factors considered when performing the risk assessment are:

- **Probability:** What is the likelihood that a threat will occur?
- **Impacts:** What are the immediate damages if the threat is realized (e.g., disclosure of information, modification of data, disruption of key systems/processes, containment, and resolution costs)?
- **Identify Information Assets:** What should be protected in relation to electronic data, IT applications and IT infrastructure? Our methodology takes into consideration any third parties or vendors that transmit, host, or process your organization's data or IT systems.
- **Criticality Analysis:** How critical are your information assets? Each technology layer (i.e., data, applications, and infrastructure) has its own unique criticality analysis.
- **Threats:** Identify the natural to man-made threats that impact the confidentiality, availability, and integrity of your data and information systems.
- **Consequences:** What are the long-term effects of the threat being realized (e.g., damage to reputation of your organization, loss of business or revenue, damage to your brand)?
- **Controls:** What effective security measures (security services and mechanisms) are needed to protect the assets?

In understanding the high risk areas for the IT applications and systems, several key questions came to mind when addressing the Cybersecurity considerations:

- What security controls are needed to satisfy the security requirements and to adequately mitigate risk incurred by using information and information systems in the execution of organizational missions and business functions?
- Have the security controls been implemented, or is there an implementation plan in place?
- What is the desired or required level of assurance that the selected security controls, as implemented, are effective in their application?

The answers to these questions are not uniquely answered in isolation but rather in the context of an overall effective risk management process suggested by the NIST Cybersecurity Framework. Through the control evaluation process, we isolated areas that City of Georgetown can continue to identify, mitigate, and monitor risks associated with cyber threats identified through the threat assessment. Logically, areas of high risk would require more extensive controls than low risk areas and in most cases, inherent risks can be controlled by the implementation of adequate countermeasures.

## APPENDIX B

### NIST Cybersecurity Framework Maturity Summary

The chart below indicates City of Georgetown's overall picture of the current state versus it's desired/target state in accordance with the Cybersecurity framework.



# Mitigation Plan

## APPENDIX B

### 3.1 FINDINGS AND RECOMMENDATIONS

3.1.1 Cybersecurity Governance Model	Assigned to:	City of Georgetown
	Priority	High
	<b>Recommendations</b>	
	<p>Currently, the City's Information Technology department has no succession plan for key roles occupied by experienced staff. In addition, most members of the IT department perform several duties beyond their originally assigned tasks and roles and responsibilities related to key initiatives such as Risk &amp; Incident Management, Disaster Recovery &amp; Business Continuity are not clearly defined.</p> <p>According to Information Security Governance Guidance for Boards of Directors and Executive Management, 2nd edition, the five basic outcomes of information security governance include:</p> <ol style="list-style-type: none"> <li>1. Strategic alignment of information security with business strategy to support organizational objectives</li> <li>2. Risk management by executing appropriate measures to manage and mitigate risks and reduce potential impacts on information resources to an acceptable level</li> <li>3. Resource management by utilizing information security knowledge and infrastructure efficiently and effectively</li> <li>4. Performance measurement by measuring, monitoring and reporting information security governance metrics to ensure that organizational objectives are achieved</li> <li>5. Value delivery by optimizing information security investments in support of organizational objectives</li> </ol> <p>At a minimum, we recommend the City implement a governance framework that allows for the proper management of a successful Information Security program (ISP). An effective ISP involves participation from senior management to set the direction for proper information security practices, adequate staffing (with assigned roles and responsibilities) and compliance with policies. Furthermore, a commitment from management helps to ensure support and funding from for security activities requiring financial resources; and that organization-wide risk management programs are developed and implemented effectively.</p> <p>Source: <a href="http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Information-Security-Governance-Guidance-for-Boards-of-Directors-and-Executive-Management-2nd-Edition.aspx">http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Information-Security-Governance-Guidance-for-Boards-of-Directors-and-Executive-Management-2nd-Edition.aspx</a></p>	

## APPENDIX B

3.1.2 Risk Management	Assigned to:	City of Georgetown
	Priority	High
	<b>Recommendations</b>	
	<p>At the City of Georgetown, it is evident that the IT department has taken measures in implementing security practices throughout the IS environment; however organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad hoc/reactive manner; an organization-wide approach to managing cybersecurity risk has not been established. As a result, security activities or business strategies may not be directly aligned with organizational risk objectives or the current threat landscape.</p> <p>The City has undertaken an effort through this assessment to evaluate the security controls needed to combat cybersecurity risks, but there is a need for an overall information security risk assessment to identify risks to the organization and threat mitigation strategies.</p> <p>To this effect, we recommend that management adopt a practice of performing a risk assessment periodically. The periodic approach may take either of the following approaches: (A) performing a full assessment every other year due to intensive resources required to facilitate such an exercise or, (B) a targeted approach done annually. The targeted approach may include:</p> <ul style="list-style-type: none"> <li>(1) revisiting Plante Moran's deliverables and updating controls where appropriate,</li> <li>(2) re-assessing the City's mitigation plan to update progress and note any further concerns, and/or</li> <li>(3) Selecting a few high-priority control areas (e.g. vendor management, or any business objective/goal identified by executive management) and re-assessing associated threats related to those areas.</li> </ul> <p>Irrespective of the approach selected, the process for performing a risk assessment typically includes:</p> <ul style="list-style-type: none"> <li>• Identification of information assets (data, applications, infrastructure, and vendors)</li> <li>• Assigning value to identified assets based on criticality (or dollar value in some cases)</li> <li>• Evaluation of vulnerabilities and threats</li> </ul> <p>In addition to the above, we also suggest that the City assess the penalties and impact of security breaches. From a regulatory perspective, such liabilities should be considered to ensure that risks to sensitive data is properly assessed and accounted for.</p> <p>Moreover assessing information security risks throughout the organization provides keen insight into management's risk tolerance for implementing security layers within the organization. The IT risk assessment should be in-line with the City's risk management strategies for identifying risks, evaluating existing controls and mitigating controls, understanding residual risk and establishing a risk mitigation plan.</p>	

## APPENDIX B

3.1.3 Policies and Procedures	Assigned to:	City of Georgetown
	Priority	High
	<b>Recommendations</b> <p>Security policies and procedures are key components of an Information Security Program. They reflect the organization's business processes and strategy, thereby enabling management to define the scope of security, what is expected from employees, dictate what must be protected and to what extent, and what the consequences of noncompliance will be. To this effect, in addition to the already existing Acceptable Use policy in place, we recommend management consider an organization-wide Information Security Policy, to include key sections such as the ones listed below:</p> <ul style="list-style-type: none"> <li>• Purpose/Scope</li> <li>• Roles and responsibilities (including those related to regulatory requirements)</li> <li>• Management commitment and business owner requirements</li> <li>• Enforcement</li> <li>• Information Sharing: Define and set requirements for relationships with or connections to information systems of other agencies.</li> </ul> <p>Additional policies that the City should consider adding include:</p> <ul style="list-style-type: none"> <li>• Data Classification</li> <li>• Information Risk Management (IRM)</li> <li>• User Access Provisioning and Review</li> <li>• Data Backup and Retention</li> <li>• Data Destruction/Retention Policy</li> <li>• Media Handling/Disposal Policy (this can be combined with the existing Computer Disposal Policy)</li> <li>• Data Protection and Encryption</li> <li>• Secure Configuration/Hardening</li> <li>• Physical Security Policy</li> <li>• Contingency Plan</li> <li>• Vulnerability Assessment and Remediation</li> <li>• Incident Response Policy (for breaches, events and other critical incidents)</li> </ul> <p>The ISP should be reviewed periodically (e.g. annually) by senior management and enforced through annual end-user acknowledgement signoffs.</p>	



## APPENDIX B

3.1.4 Asset Management: Data Classification		Assigned to:	City of Georgetown
		Priority	High
	Recommendations		
	<p>The City has identified and catalogued its hardware and software via a tool called Lansweeper. This approach ties into an overall information flow enforcement (<b>NIST SP 800-53</b> Rev. 4 AC-4) which ensures the confidentiality, integrity, and availability of critical data when defined and enforced.</p> <p>The next step is to classify data within the system based on its criticality and / or sensitivity (<b>NIST SP 800-53</b> Rev. 4 RA-2). Classification of data will also help drive the above-mentioned information flow enforcement and help define the City's security architecture. Most organizations conduct the security categorization process as an organization-wide activity with the involvement of chief information officers, senior information security officers, information system owners, mission/business owners, and information owners/stewards.</p> <p>Plante Moran recommends the classification of City data to define an appropriate set of protection levels and communication required for special handling. Classifications and associated protective controls (including encryption for data at rest and data leak prevention tools) should take into account department needs for sharing or restricting information and the associated business impacts if such data were compromised. Successful data classification in an organization requires a thorough understanding of where the organization's data assets reside and on what applications/devices they are stored. Handling procedures should include details regarding the secure processing, storage, transmission, declassification, and destruction of data.</p>		

## APPENDIX B

3.1.5 Access Management	Assigned to:	City of Georgetown
	Priority	High
	Recommendations	
	<p><b>Logical Access:</b> Access provisioning to the system is completed on the practice of mirroring, that is, 'set up as another user within the system'. This practice can potentially lead to excessive access rights being provided to users. On the other hand, for existing users, additional access is provisioned without a formal review for SoD (Segregation of Duties) conflict. When users are terminated, access removal from all necessary applications may not be performed in a timely manner due to delayed notification from HR to the IT department. Furthermore, in all aforementioned scenarios (access provisioning, modification and termination), it was noted that not all applications have a formal process of provisioning and de-provisioning.</p> <p>A role-based access scheme should be established to ensure consistent application of user access rights within the system. Users should be assigned their base set of access authorizations based on the concept of "Least Privilege Necessary" to perform their role or job function (as defined within their formal job description). Additional access beyond the previously established role-based access scheme should be formally requested, reviewed for conflicts and approved (<b>NIST SP 800-53</b> Rev. 4 AC-2). Moreover, Management should consider integrating access rights with data classification efforts identified in the findings within this report (See 3.1.4 above, for more details).</p> <p><b>Physical Security:</b> The City currently monitors physical access to the facility where information system resides to detect and respond to physical security incidents. However, CoG does not review physical access logs periodically (e.g. quarterly/annually).</p> <p>We recommend management take the following actions:</p> <ol style="list-style-type: none"> <li>1. Establish a role based access scheme that takes into account the job responsibilities associated with each role for City of Georgetown.</li> <li>2. Establish a process to periodically review user access (including physical access) to ensure accuracy and adherence to existing/changed business processes.</li> <li>3. Ensure a process is in place to approve additional or special access requests and timely de-provision access upon notification from HR.</li> <li>4. Implement and enforce procedures to identify and document appropriate access requirements for removing, adding or modifying City personnel's access to electronic PHI. The need for and extent of access should be based on an assessment of risk, cost, benefit and feasibility as well as business need, and permission to view, alter, retrieve and store ePHI.</li> <li>5. Perform a periodic review of user access to PHI and ePHI (including access to the data center) to verify the list is accurate and to ensure access is still commensurate with job responsibilities.</li> </ol>	

## APPENDIX B

3.1.6 Contingency Plan	Assigned to:	City of Georgetown
	Priority	High
	Recommendations	
	<p>In order to ensure that critical operations are available in the event of an interruption or incident, redundancy is built into the datacenter environmental controls at the City and an extensive data backup strategy is in place. However, a formal contingency plan is not in place and related resources/systems are not catalogued and prioritized.</p> <p>Plante Moran recommends the City conduct and formalize:</p> <p>(1) a Business Impact Analysis (BIA) which identifies and analyzes mission-critical business functions, and then quantifies the impact a loss of those functions would have on the City, and</p> <p>(2) An information system contingency plan to mitigate the risk of critical system and service unavailability. The contingency planning process should occur after a formal Business Impact Analysis (BIA) is conducted, in order to correlate the system with the critical processes and services provided, and based on that information, characterize the consequences of a disruption. Three steps are typically involved in accomplishing the BIA:</p> <ul style="list-style-type: none"> <li>• Determine mission/business processes and recovery criticality</li> <li>• Identify resource requirements</li> <li>• Identify recovery priorities for system resources</li> </ul> <p>The information system contingency plan should consider three phases:</p> <p>(1) Activation and Notification Phase which outlines activation criteria and notification procedures,</p> <p>(2) Recovery Phase which outlines recovery activities, escalation, and notification, and</p> <p>(3) Reconstitution Phase which allows validating successful recovery and deactivation of the plan through activities such as validation testing, notifications, and event documentation.</p> <p>The contingency planning process should also include the following elements:</p> <ul style="list-style-type: none"> <li>• Roles and responsibilities</li> <li>• Scope as applies to common platform types and organization functions (i.e., telecommunications, legal, media relations)</li> <li>• Resource requirements</li> <li>• Training requirements</li> <li>• Exercise and testing schedules</li> <li>• Plan maintenance schedule, and</li> <li>• Minimum frequency of backups and storage of backup media</li> </ul> <p>Further, an effective contingency plan should tie into the City's Incident Response Plan and should consider City's personnel as information system contingency plans are not executed on their own and an incident will often impact individuals that are crucial to tasks related to information system operations. Personnel safety and evacuation, personnel health, personnel welfare, relationships with response organizations, and communication planning should be considered when developing the contingency plan. Finally, the agreed upon plan should be compatible with the enterprise-wide Business Continuity Plan.</p> <p>Sources: <a href="http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf">http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf</a></p>	

## APPENDIX B

3.1.7 Incident Response Management	Assigned to:	City of Georgetown
	Priority	High
	<b>Recommendations</b>	
	<p>Based on inquiry, it was noted that the City of Georgetown does not have a formal Incident Response Plan. Incident management includes a proactive and reactive phase. While reactive measures help to ensure that incidents are properly handled, proactive measures allow incidents to be detected in a timely and controllable manner (<b>See finding 3.1.9</b>). An improved approach will be to implement an Incident Management Program, which is initiated by an Incident Response Policy and include the following key elements:</p> <ul style="list-style-type: none"> <li>• Provide a roadmap for implementing its incident response capability;</li> <li>• Describes the structure and organization of City of Georgetown's incident response capability;</li> <li>• Provides a high-level approach for how the incident response capability fits into City of Georgetown as a whole and the overall Family of Companies;</li> <li>• Meets the unique requirements of City of Georgetown's mission, size, structure, and functions;</li> <li>• Defines reportable incidents as well as ;</li> <li>• Requirements and guidelines for external communications and information sharing (e.g., what can be shared with whom, when, and over what channel)</li> <li>• Provides metrics for measuring the incident response capability within the organization;</li> <li>• Defines the resources and management support needed to effectively maintain and mature an incident response capability; and</li> <li>• Is reviewed and approved by senior management</li> </ul> <p>We recommend management take the following actions:</p> <ol style="list-style-type: none"> <li>1. Develop a more comprehensive plan incorporating the above elements.</li> <li>2. Integrate City of Georgetown's Incident Response Plan testing activities with relevant third parties.</li> </ol>	

## APPENDIX B

3.1.8 Third Party Cybersecurity Roles & Responsibilities	Assigned to:	City of Georgetown
	Priority	High
	<b>Recommendations</b> <p>While the City has identified trusted partners with respect to hardware and hosted applications. We noted the following deficiencies related to third party roles and responsibilities:</p> <ul style="list-style-type: none"> <li>• The contract between City of Georgetown and the service provider does not specifically outline the roles and responsibilities related to Cybersecurity controls handled by each organization.</li> <li>• There is no monitoring of external party use of the system for potential Cybersecurity events.</li> </ul> <p>Security roles and responsibilities should be established for all third-party service providers (<b>NIST SP 800-53</b> Rev. 4 PS-7). Responsibilities are key to ensure that the City of Georgetown and its service providers understand exactly who is responsible for which Cybersecurity controls; this is especially important in a business continuity situation. These roles and responsibilities should be formally documented in a contractual agreement.</p> <p>Service level agreements should be established based on Key Performance Indicators (KPI) where City of Georgetown's expectations are set for each outsourced responsibility to its third-party service providers. Once established, KPIs should be monitored to ensure third-party service providers adhere to contractual obligations (<b>NIST SP 800-53</b> Rev. 4 CA-7). Furthermore, adherence to Key Performance Indicators should be used to identify potential issues with vendor service that can be addressed through negotiations or seeking a new vendor.</p> <p>We recommend management take the following actions:</p> <ol style="list-style-type: none"> <li>1. Clearly identify the cybersecurity responsibilities to be outlined in the contract with the service provider including roles for identification, response, and recovery procedures.</li> <li>2. Establish Key performance indicators for third-party responsibilities including number of events, data breaches, number of notifications.</li> <li>3. Continuously monitor established key performance indicators.</li> </ol>	

## APPENDIX B

3.1.9 Critical Security Event Identification	Assigned to:	City of Georgetown
	Priority	Medium
	<b>Recommendations</b>	
	<p>We noted a variety of log generation methods are in place for the system. These logs can be used to identify everything from system health to potential security violations. Presently, there is not a comprehensive catalog of security related event types being identified and reviewed within the logs by security professionals.</p> <p>To establish an effective event logging and monitoring program, City of Georgetown will need to first identify high risk events that can be alerted from current logging capabilities (<b>NIST SP 800-53</b> Rev. 4 AU-6). Potential high risk events can be discerned through the risk assessment process (<b>NIST SP 800-53</b> Rev. 4 RA-3), penetration testing, and best practice documentation. Some common threat events include:</p> <ul style="list-style-type: none"> <li>• Multiple failed login attempts</li> <li>• Elevations in access privileges</li> <li>• Changes to application code</li> <li>• Changes to security settings</li> <li>• Process specific actions</li> </ul> <p>For more risky events, such as devices that connect to the network without authorization, the organization may consider alert generation techniques while for less risky events they may simple review on a periodic basis. Identified events should be responded to in accordance with the organization's Incident Response Plan (<b>NIST SP 800-53</b> Rev. 4 IR-4, IR-5).</p> <p>Once event detection processes are implemented a process to test said processes should be established. Security assessments by internal or external independent parties can be an effective way to ensure logging and monitoring processes are effective (<b>NIST SP 800-53</b> Rev. 4 CA-2). Management should seek continuous improvement opportunities for the event logging and monitoring program based on the results of security assessments.</p> <p>We recommend management take the following actions:</p> <ol style="list-style-type: none"> <li>1. Identify the system events that may indicate a potential security event.</li> <li>2. Define monitoring techniques commensurate with associated risk.</li> <li>3. Establish formal policies and procedures related to defined monitoring activities.</li> <li>4. Periodically test the effectiveness of event logging and monitoring processes.</li> </ol>	

## APPENDIX B

3.1.10 Security Awareness, Training and Education	Assigned to:	City of Georgetown
	Priority	Medium
	<b>Recommendations</b>	
	<p>The City has implemented an acceptable use policy amongst other policies around proper use of computers and accessing digital information. However, to ensure compliance, there is a need to assess employee's understanding of policies and response to cybersecurity threats via periodic awareness and training.</p> <p>End users are the first line of defense against a variety of social engineering threats and must be relied upon to appropriately select strong passwords, perform secure day-to-day operations, and appropriately use equipment. By not providing formal training to all employees, the risk is increased that employees may not follow appropriate security procedures.</p> <p>We recommend a formal IT security awareness training be provided to all employees on a periodic basis. Employees should be educated on the organization's information security policies upon hire, periodically (at least annually), and as major changes occur. In addition, employees should be required to formally acknowledge that they have read and understand the security topics discussed, and that they understand the ramifications of noncompliance. Management should consider allocating resources for security awareness activities (including other items, e.g. banners and posters), and enforce employee participation/attendance within the organization.</p>	

## APPENDIX B

3.1.11 Unauthorized Mobile Code Detection		Assigned to:	City of Georgetown
		Priority	Low
	<b>Recommendations</b>		
	<p>Mobile code is defined as any program, application, or content that is capable of being embedded and transferred (via email, document, website, etc.). Examples of mobile code include: JavaScript, Active X, PDF, VBscripts, etc. Avenues There are currently multiple avenues for mobile code to be introduced into the information systems supporting the system. Mobile code may be introduced from USB (current USB restriction only prevent data being copied to a USB), through email, and through downloads from websites.</p> <p>The City should identify the types of mobile code that are approved for use within the information system and educate users on the proper use of related technologies. Likewise, organizations should define which types of mobile code are not approved for use within the information system. Processes should be defined to identify unauthorized mobile code deployed within the environment. These processes could include configuration management controls, vulnerability scanning, etc. (<b>NIST SP 800-53 Rev. 4 SC-18</b>).</p> <p>City of Georgetown does have controls in place to mitigate the risk of malicious mobile code: antivirus controls, and limiting user access to administrator functions based on the concept of least privilege.</p> <p>We recommend management take the following actions:</p> <ol style="list-style-type: none"><li>1. Define acceptable and unacceptable mobile code and mobile code technologies.</li><li>2. Deploy a process to monitor for the presence of mobile code</li><li>3. Integrate mobile code detection processes into the Incident Response Plan</li></ol>		





plante moran | Audit. Tax. Consulting.  
Wealth Management.

**Doug Farmer**

Engagement Partner

3125-602-3691

[doug.farmer@plantemoran.com](mailto:doug.farmer@plantemoran.com)

City of Georgetown, Texas  
Government and Finance Advisory Board  
October 28, 2020

**SUBJECT:**

Consideration and possible action to recommend a resolution formally adopting the City's Investment Policies for Fiscal Year 2021 – Leigh Wallace, Finance Director

**ITEM SUMMARY:**

This item is to recommend the Investment Policy to City Council. The purpose of the Investment Policy is to provide the framework for managing the City's investments in a way that mitigates risk while optimizing returns. The policy is modeled after Public Funds Investment Act (PFIA) recommendations. According to the Act, the Council must approve the policies annually. The City's Investment Advisors, Valley View Consulting, and City staff worked together on the updates. There are no major updates for FY2021.

**FINANCIAL IMPACT:**

.

**SUBMITTED BY:**

Sharon A Parker

**ATTACHMENTS:**

<b>Description</b>		<b>Type</b>
<input type="checkbox"/>	Investment Policy Presentation	Presentation
<input type="checkbox"/>	Investment Policy FY2020-2021 Recommended	Backup Material
<input type="checkbox"/>	Investment Policy Resolution	Resolution Letter

# Investment Policy Review and Portfolio

## ► Summary

GGAF

October 2020

# PFIA Requirements

- ▶ Public Funds Investment Act, Texas Government Code Chapter 2256
- ▶ Requires written investment policy that meets requirements
- ▶ Investment policy
  - ▶ Must be approved by Council
  - ▶ Must be reviewed annually by Council
- ▶ Investment strategies & objectives must be outlined
- ▶ Investment officers must be designated
- ▶ Mandates training for investment officers

# PFIA Requirements

- ▶ Specifies the type of securities allowed
  - ▶ No derivatives
  - ▶ City policy can be and is more restrictive
- ▶ Safekeeping and Custody
  - ▶ Authorized brokers/dealers
  - ▶ Competitive bid process
  - ▶ Collateral minimum 102%
- ▶ Regular reporting of investments
  - ▶ Minimum information items required
- ▶ Compliance audit as part of annual financial audit
  - ▶ Focus on management controls and adherence to approved investment policy
  - ▶ Quarterly investment report reviewed

# Investment Policy Objectives

*In priority order*

Safety-Preservation and safety of principal

Liquidity-Sufficient cash to pay obligations when due

Public Trust-No investments that may be questionable by public

Yield-Maximize earnings within policy

# City's Authorized Investments

- ▶ Financial Institution Deposits
- ▶ US Treasuries and Agencies
- ▶ Investment Pools
  - ▶ AAA Rated & Mark to Market daily
- ▶ Money Market Mutual Funds
- ▶ Repurchase Agreements
- ▶ Texas Municipal Issuers
  - ▶ Rated "A" or better

# Investment Policy Compliance

- ▶ Certified by the Government Treasurers Organization of Texas (GTOT)
  - ▶ Best practices - model policy guidelines
- ▶ Part of Independent Auditor's work
  - ▶ Review for compliance with all legal requirements
  - ▶ Opinion Letter in Comprehensive Annual Financial Report (CAFR)



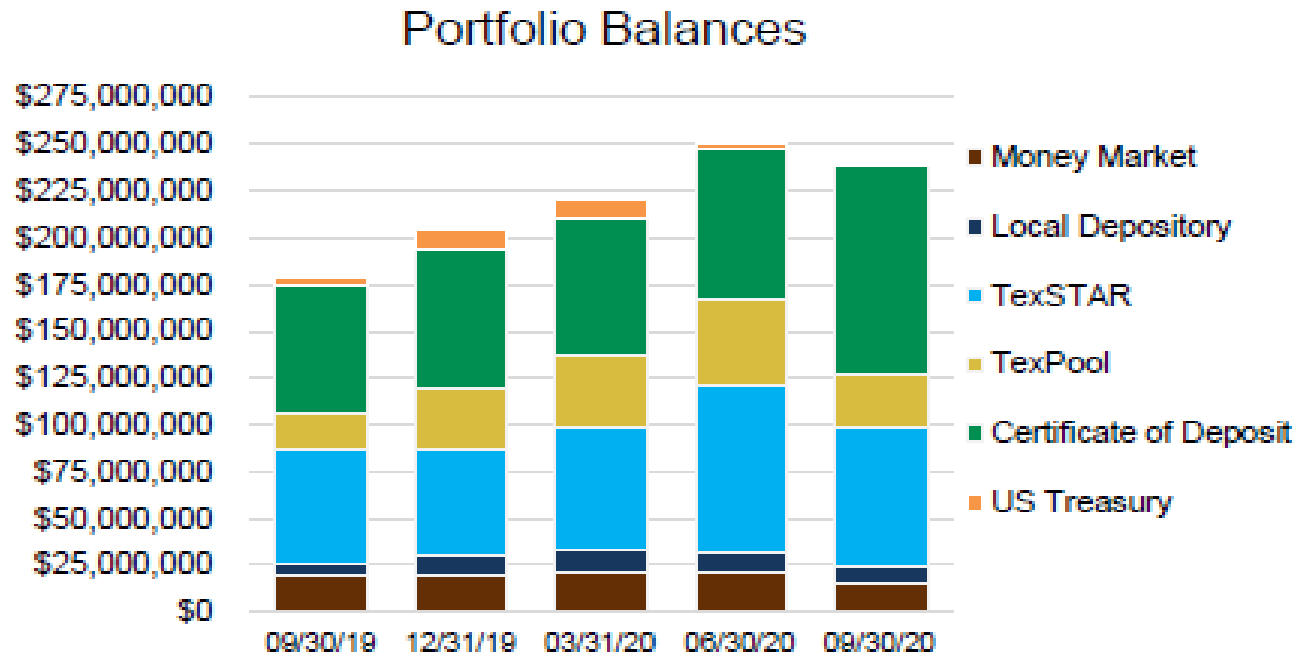
# Review Proposed Changes

Add	Add Investment Officer - Assistant Finance Director
Edit	Minor editing changes <ul style="list-style-type: none"><li>• Broker/Dealer List</li></ul>
Monitor	Staff will continue to monitor for policy issues and federal & state law changes

# Year in Review - 2020

- ▶ Interest earnings declined drastically in 2020.
  - ▶ Due to COVID-19 and market changes, the Fed Rate decreased significantly in 2020 to 0-.25%.
  - ▶ Example: In August 2019, we accepted a rate of 2.25%, but in September 2020, our highest rate was .30% for 9 months.
- ▶ Continued laddered purchases throughout the year.
- ▶ Renewed Depository Banking Contract through Spring 2022.

# City Portfolio-Type By Quarter



# Investment Strategy



**REVIEW CASH FLOW  
NEEDS**



**MAINTAIN PROJECT  
SCHEDULE FOR BOND  
PROCEEDS**

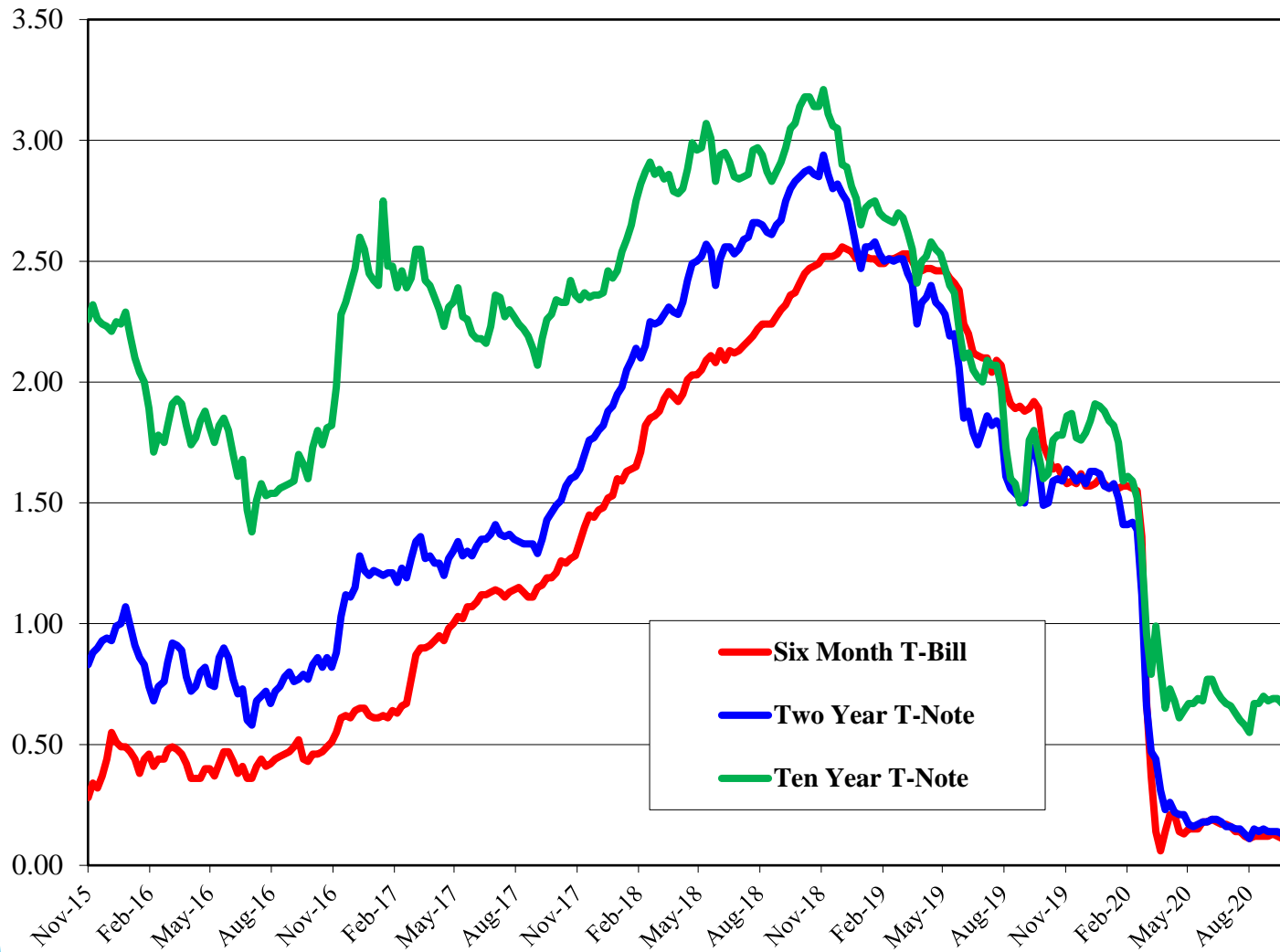


**INVEST ON A LADDERED  
APPROACH**

# Market Update

Susan Anderson  
Valley View Consulting, L.L.C.  
City's Investment Advisor

## US Treasury Historical Yields - Since Nov 2015



# Next Steps:

- 1. Policy as presented along with any GGAF changes will be on the December 8, 2020 Council agenda.
- 2. Ongoing quarterly reports to Council.

# Investment Policy Review

Questions/Comments



**CITY OF GEORGETOWN, TEXAS  
INVESTMENT POLICY  
As amended December 8, 2020**

**SECTION 1: SCOPE & OBJECTIVES**

**1.1 SCOPE**

This Investment Policy applies to all financial assets of the City of Georgetown, Texas, which includes the City of Georgetown Economic Development Corporation and the Georgetown Transportation Enhancement Corporation, held in all funds.

**1.2 STATEMENT OF CASH MANAGEMENT PHILOSOPHY**

The City will maintain a comprehensive cash management program to include the effective collection of all accounts receivable, the prompt deposit of receipts to the City's bank accounts, the payment of obligations to comply with State law and in accord with vendor invoices, and the prudent investment of idle funds in accord with this Policy.

**1.3 OBJECTIVES**

The City's investment program will be conducted to comply with Texas Government Code Chapter 2256 (the Public Funds Investment Act) and accomplish the following objectives, listed in priority order:

1. *Safety.* The City will give priority to the preservation and safety of the principal invested. Investments will be made in a manner that will mitigate credit risk and interest rate risk.
2. *Liquidity.* The City will maintain the availability of sufficient cash to pay obligations of the City when they are due.
3. *Public Trust.* Investment Officers shall seek to act responsibly as custodians of the public trust. Investment Officers shall avoid transactions that might impair public confidence in the City's ability to govern effectively.
4. *Yield.* The City will invest idle cash in a manner that will maximize earnings to the greatest extent possible, consistent with State and local laws and the objectives of safety and liquidity listed above.

It is also the objective of the City to diversify its investments to eliminate the risk of loss resulting from over concentration of assets in a specific maturity, a specific issuer or a specific class of investments, when appropriate. It is the intent of the City to hold investments to maturity.

**SECTION 2: STANDARD OF CARE**

**2.1 PRUDENCE**

Investments will be made with judgment and care, under prevailing circumstances, that a person of prudence, discretion, and intelligence would exercise in the management of the person's own affairs, not for speculation, but for investment, considering the probable safety of capital and the probable income to be derived. The City Council recognizes that in maintaining a diversified portfolio, occasional measured losses due to market volatility are inevitable and must be

considered within the context of the overall portfolio's investment return, provided that adequate diversification has been implemented.

In determining whether an Investment Officer has exercised prudence with respect to an investment decision, the determination shall be made taking into consideration:

- A. The investment of all funds, or funds under the City's control, over which the Officer had responsibility rather than a consideration as to the prudence of a single investment.
- B. Whether the investment decision was consistent with the written Investment Policy of the City.

The Investment Officers, acting in accordance with written procedures and exercising due diligence, shall not be held personally responsible for a specific investment's adverse credit risk or market price changes, provided that these deviations are reported immediately to the City Manager and/or the City Council and that appropriate action is taken to control adverse developments.

## **2.2 ETHICS & CONFLICT OF INTEREST**

Investment Officers and employees involved in the investment process will refrain from personal business activity that could conflict with the proper execution of the investment program, or which could impair their ability to make impartial investment decisions. Investment Officers and employees will comply with all disclosure and reporting requirements of Section 2256.005 (i) of the Texas Government Code.

## **2.3 DELEGATION OF AUTHORITY**

The Finance Director, both Assistant Finance Directors, and the Treasurer are the City's Investment Officers. The Finance Director is responsible for overall management of the City's investment program and may direct the other Investment Officers in his/her duties. Accordingly, the Investment Officers are responsible for day-to-day administration of the investment program and for the duties listed below:

- 1. Maintain current information as to available cash balances in City accounts, and as to the amount of idle cash available for investment;
- 2. Make investments and maintain written procedures for the operation and internal control of the investment program consistent with this Policy;
- 3. Ensure that all investments are adequately secured; and
- 4. Attend training relating to investment responsibilities under this Policy as required by Section 2256.008 of the Texas Government Code. Ten (10) hours of investment training must be completed within twelve (12) months of attaining the position of Investment Officer, and thereafter, eight (8) hours of training must be completed within a two-year period that begins on the first day of the City's fiscal year and consists of the two consecutive fiscal years after that date. To ensure quality and capability of investment management, all Investment Officers shall receive training from an independent source that addresses investment controls, security risks, strategy risks, market risks, diversification of investment portfolios, and compliance with the Public Funds Investment Act. The Training sponsored by any of the following organizations is approved:

Texas Municipal League

Government Finance Officers Association of Texas (GFOAT)  
Government Finance Officers Association of the United States and Canada  
Government Treasurers' Organization of Texas (GTOT)  
University of North Texas  
Texas Tech University Center for Professional Development

Unless authorized by law, no person may deposit, withdraw, transfer or manage in any other manner the funds of the City.

## **SECTION 3: INVESTMENT STRATEGIES**

### **3.1 OPERATING FUNDS**

Operating Funds are defined as cash and investments used for day-to-day operations that do not fall into one of the other categories. Operating Funds will be invested in a manner suitable to provide adequate liquidity for the anticipated operating needs of the City. Investments of Operating Funds shall be limited to a weighted average maturity no greater than one year and any one investment may not exceed 36 months without authorization by the City Manager. All investment instruments must meet credit and safety criteria as required by the Public Funds Investment Act and this Policy. All investments shall be of high quality with no perceived default risk. Operating Funds will remain sufficiently liquid to enable the City to meet operating requirements that may be reasonably anticipated. If utilized, securities with active and efficient secondary markets are necessary in the event of unanticipated cash requirements. Operating Funds' maturities will be staggered based on the City's anticipated operating needs, and the investments may include financial institution deposits, U.S. treasuries and agencies, state and municipal debt instruments, investment pools, and money market mutual funds. Investment of Operating Funds will be structured to attain the optimal yield given the liquidity and safety requirements.

### **3.2 CONTINGENCY RESERVES (or operating reserves)**

Contingency Reserves are the minimum fund balance/working capital requirements as defined by City Council in the Annual Operating Plan. Contingency Reserves' balances may be used to cover any cash operating shortfalls due to the timing of bond issues, revenue receipts, etc. The funds will be invested in a manner suitable to cover operating shortfalls that may be reasonably anticipated. All investment instruments must meet credit and safety criteria as required by the Public Funds Investment Act and this Policy. All investments shall be of high quality with no perceived default risk. Investments of these funds may exceed 24 months with prior approval of the City Manager if short term cash flow needs are not evident. Any one investment may not exceed 36 months in maturity length. The weighted average maturity for these funds may not exceed 24 months. Contingency Reserves investments will remain sufficiently liquid to meet City needs in the event of an operating shortfall, and if utilized, securities with active and efficient secondary markets will provide marketability necessary should the need arise to liquidate the investment prior to maturity. Contingency Reserves' maturities will be diverse to cover possible operating shortfalls, and the investments may include financial institution deposits, U.S. treasuries and agencies, state and municipal debt instruments, investment pools, and money market mutual funds. Investment of Contingency Reserves will be structured to attain the optimal yield given the liquidity and safety requirements.

### **3.3 DEBT**

**3.3.1 Reserves.** Debt Reserves are defined as bond reserve funds required to be set aside in accordance with bond covenants. The City's bond covenants do not require the City to maintain any reserve funds. Therefore, the City's investments are not adversely affected by any reserve requirement conditions.

**3.3.2 Interest & Sinking (or debt service funds).** Interest and Sinking funds are defined as those funds accumulated to meet periodic payments required by bond and note maturity schedules. The investment maturities are limited by pertinent debt service requirements and tax laws limiting accumulation and earnings for such funds, and investments should be made in a manner suitable to comply with applicable requirements and payment schedules. The investments must meet credit and safety criteria as required by the Public Funds Investment Act and this Policy. All investments shall be of high quality with no perceived default risk. The funds shall be invested to ensure adequate funding for each consecutive debt service payment but shall not exceed the debt service schedule. Involuntary liquidation of investments is highly unlikely due to the nature of these funds. Interest and Sinking fund maturities will be diversified by matching them to the debt service payments of the City, and the investments may include financial institution deposits, U.S. treasuries and agencies, state and municipal debt instruments, investment pools, and money market mutual funds. Investment of Interest and Sinking funds will be structured to attain the optimal yield given the liquidity and safety requirements.

### **3.4 BOND PROCEEDS (capital improvement funds)**

Bond proceed funds are defined as those funds received from the sales of City bonds or notes and not otherwise set aside for debt service or reserve purposes. These funds typically include money to fund infrastructure, construction, or other large projects. The investment maturities are limited by pertinent project draw requirements, applicable bond covenants, and tax laws governing earnings for such funds, but may not have a single security greater than 36 months, unless a flexible repurchase agreement is used in accordance with Section 4.1.5 of this Policy. Investments must meet credit and safety criteria as required by the Public Funds Investment Act and this Policy and should be made in a manner suitable to meet project requirements. All investments shall be of high quality with no perceived default risk. The funds shall be invested to match projected cash flow requirements with sufficient liquidity to meet unanticipated project outlays, and maturities shall not exceed the expected project completion dates. Bond proceed maturities will be diverse to provide necessary liquidity based on project needs, and investments may include financial institution deposits, flexible repurchase agreements, U.S. treasuries and agencies, state and municipal debt instruments, investment pools, and money market mutual funds. Investment of Bond Proceeds will be structured to attain the optimal yield given the liquidity and safety requirements.

## **SECTION 4: AUTHORIZED INVESTMENTS**

### **4.1 AUTHORIZED INVESTMENTS**

City funds may be invested in the following authorized investments:

**4.1.1 Financial Institution Deposits.** Certificates of Deposit and other evidences of deposit at a financial institution that, a) has its main office or a branch office in Texas and is guaranteed or insured by the Federal Deposit Insurance Corporation or its successor, b) is secured by obligations or in any other manner and amount provided by law for deposits of the City, or c) is executed through a depository institution or approved broker that has its main office or a branch office in Texas that meets the requirements of the Public Funds Investment Act. All financial institution deposits in excess of the FDIC insured amount must be collateralized as described by Section 5.5 COLLATERALIZATION.

**4.1.2 U.S. Treasuries and Agencies.** Obligations of the United States of America, its agencies and instrumentalities, including other obligations, the principal and interest of which are unconditionally guaranteed or insured by, or backed by the full faith and credit of the United States or its agencies and instrumentalities, including obligations that are fully guaranteed or insured by the Federal Deposit Insurance Corporation or by the explicit

full faith and credit of the United States. Such obligations include letters of credit of the United States or its agencies and instrumentalities, including the Federal Home Loan Banks.

**4.1.3 Investment Pools.** Investment pools that meet all requirements of the Public Funds Investment Act, including the following criteria:

- a. An investment pool must provide an offering circular or other similar disclosure instruments and provide monthly and transaction reporting as required by Section 2256.016 of the Texas Government Code.
- b. Investment in a new pool will require the approval of the City Council.
- c. A public funds investment pool created to function as a money market mutual fund must (1) mark its portfolio to market daily, (2) include in its investment objectives the maintenance of a stable net asset value of \$1.00 for each share and (3) be continuously rated no lower than AAAm or at an equivalent rating by at least one nationally recognized rating service.

**4.1.4. Money Market Mutual Funds.** No-load government money market mutual funds if the fund:

- a. Is compliant with the Public Funds Investment Act;
- b. Is regulated by the Securities and Exchange Commission;
- c. Marks its portfolio to market daily;
- d. Includes in its investment objectives the maintenance of a stable net asset value of \$1.0000 for each share;
- d. Is continuously rated no lower than AAA or at an equivalent rating by at least one nationally recognized rating service.

**4.1.5. Repurchase Agreements.** Fully collateralized repurchase agreements that:

- a. Have a defined termination date;
- b. Are secured by cash or obligations as allowed by the Public Funds Investment Act and this Policy;
- c. Require independent third-party safekeeping of all securities prior to the release of any funds;
- d. Are placed through a primary dealer or financial institution doing business in Texas; and
- e. Do not create a reverse repurchase agreement by the City.

Construction, capital improvement and bond proceed funds may utilize a flexible repurchase agreement, or similar agreement, that allows expenditure-related withdrawal of funds, without penalty, with an average life and termination date limitation based on the anticipated draw schedule. Any repurchase agreement shall require the execution of a mutually acceptable Repurchase Agreement.

**4.1.6. Municipal Issuers.** Obligations of:

- a. The State of Texas or its agencies and instrumentalities; and
- b. Counties, cities, and other political subdivisions of the State of Texas rated as to investment quality by a nationally recognized investment rating firm not less than A or its equivalent.

Investments purchased prior to this Policy's revision, that do not meet the revised requirements of this Policy, are not required to be liquidated. The City shall monitor each investment's status to determine whether it is in the best interest of the City to hold or liquidate the investment.

## **4.2 CREDIT RATING REVIEW AND EFFECT OF LOSS OF REQUIRED RATING**

Not less than quarterly, the Investment Officers will obtain from a reliable source the current credit rating for each held investment that has a Public Funds Investment Act-required minimum rating. Any Authorized Investment that requires a minimum rating and does not qualify at any time during the period, is considered to not have the minimum rating. The City shall take all prudent measures that are consistent with this Policy to liquidate an investment that does not have the minimum rating.

## **4.3 COMPLIANCE WITH STATE LAW**

All authorized investments outlined above must meet the requirements of the Public Funds Investment Act. No investment may be made in any instrument except as provided above.

## **4.4 CASH ON HAND**

Cash resources required for the immediate needs of the City, and not otherwise available for longer term investment, will be placed in account(s) at the City's Depository/Depositories, in local government investment pools and/or money market mutual funds. Such account(s) will earn interest at the highest rate(s) provided in the respective depository contract(s).

# **SECTION 5: SAFEKEEPING AND CUSTODY**

## **5.1 AUTHORIZED BROKER/DEALERS and INVESTMENT POLICY CERTIFICATION**

Authorized investment securities may be purchased only through brokers/dealers who are licensed and in good standing with the Texas State Securities Board, the Securities Exchange Commission, the Financial Industry Regulatory Authority, or other applicable self-regulatory organization. The City Council will, at least annually, review, revise, and adopt a list of broker/dealers who are authorized to engage in investment transactions with the City. The list is approved and included in Attachment "A" of this Policy.

Before engaging in investment transactions with an Investment Pool or discretionary investment management firm, the Investment Officers will have received from said pool/firm a signed Certification Form. This form will attest that the individual responsible for the City's account with that pool/firm has received and reviewed the City's Investment Policy and that the pool/firm has implemented reasonable procedures and controls to preclude transactions conducted between the City and the pool/firm that are not authorized by the City's Investment Policy, except to the extent that this authorization is dependent on an analysis of the makeup of the City's entire portfolio, requires an interpretation of subjective investment standards, or relates to investment transactions of the City that are not made through accounts or other contractual arrangements over which the pool/firm has accepted discretionary investment authority. The letter must be signed by a Qualified Representative as defined by the Public Funds Investment Act.

**"Qualified Representative"** means a person who holds a position with a business organization who is authorized to act on behalf of the business organization and who is one of the following:

(1) for an investment pool, the person authorized by the elected official or board with authority to administer the activities of the investment pool to sign the written instrument on behalf of the investment pool, or

(2) for a discretionary investment management firm registered under the Investment Advisers Act of 1940 or, if not subject of registration under the Act, registered with the State Securities Board, a person who is an officer or principal of the investment management firm.

## **5.2 AUTHORIZED FINANCIAL INSTITUTIONS**

Financial institution deposits and other evidences of deposit may be purchased at qualified City Depositories and other financial institutions. Qualifications will be determined by the Investment Officers. The City must have a written agreement with the Depository and other financial institutions, and that depository and other financial institutions must meet all State Laws for deposit of public funds. The City's main operating Depository/Depositories will be selected as provided by law and the City's purchasing procedure.

## **5.3 INTERNAL CONTROLS**

The Finance Director will establish and maintain procedures for the execution of the investment program and these procedures will address internal controls to mitigate risks of intentional or inadvertent mismanagement or misappropriation of funds.

All investment transactions will be documented by the Investment Officers. The Investment Officers, or through the City's Investment Advisor, may make investments orally, but will follow promptly with a written confirmation to the financial institution or broker/ dealer, with a copy of such confirmation retained in the City's files.

All trades, purchases, and sales, excluding cash equivalent transactions, will be completed through a competitive process. Where appropriate, at least three (3) quotations will be solicited for each such investment made.

Market value of the portfolio and each investment will be monitored at least quarterly through industry standard publications/sources for market data such as, but not limited to, The Wall Street Journal or Bloomberg.

## **5.4 SAFEKEEPING**

All securities purchased by the City under this Policy must be designated as assets of the City, must be settled on a delivery-versus-payment (DVP) basis, and must be protected through the use of a third-party custody/safekeeping agent. The City will enter into a formal agreement with an institution of such size and expertise as is necessary to provide the services needed to protect and secure the investment assets of the City.

## **5.5 COLLATERALIZATION**

To the extent not insured by federal agencies that secure deposits, City funds (including financial institution deposits and CDs) must be collateralized in compliance with the Texas Public Funds Collateral Act and pertinent federal banking regulations. With the exception of deposits secured with irrevocable letters of credit at 100% of deposit plus accrued interest, the aggregate market value of pledged securities shall be equal to at least one hundred two percent (102%) of the deposit plus accrued interest less an amount insured by the Federal Deposit Insurance Corporation. Should the depository fail to adequately maintain the required collateral level, the City may increase the minimum to 110%. The City reserves the right, in its sole discretion, to accept or reject any form of insurance or collateral pledged towards its deposits. Institutions serving as a depository will be required to sign a Depository/Collateral Agreement with the City. The collateralized deposit portion of the Agreement shall define the City's rights to the collateral in case of default, bankruptcy, or closing and shall establish a perfected security interest in compliance with Federal and State regulations, including:

- The agreement must be in writing;
- The agreement must be executed by the Depository and the City contemporaneously with the acquisition of the asset;
- The agreement must be approved by the Board of Directors or designated committee of the Depository and a copy of the meeting minutes must be delivered to the City; and
- The agreement must be part of the Depository's "official record" continuously since its execution.

Securities pledged as collateral must be retained by an independent, third party custodian and marked as pledged to the City. The City will be provided the original safekeeping receipt from the custodian on each pledged security. With the exception of the Federal Reserve Bank, the City, financial institution, and the custodian will operate in accordance with an acceptable custodial agreement. The City's Investment Officers must approve in writing the release of collateral prior to its removal from the safekeeping account in accordance with the terms of the depository and/or custodial agreement.

The financial institution(s) with which the City invests and/or maintains deposits will require the custodian to provide monthly a listing of the collateral pledged to the City marked to current market prices. The listing will include total pledged securities itemized by name, CUSIP, type and description of the security; safekeeping receipt number; par value; current market value; maturity date; and Moody's or Standard & Poor's rating, if available.

## **SECTION 6: REPORTING**

### **6.1 QUARTERLY REPORTING**

The Investment Officers shall prepare, sign and submit to the City Council a quarterly report on investment transactions for all funds covered by this Policy. The report will be prepared in compliance with the Public Funds Investment Act. The report will cover the investment position of the City at the end of each fiscal quarter. The contents will include at a minimum:

1. Beginning and ending market value and accrued interest of the portfolio;
2. Beginning and ending market value and book value, maturity date, type of funds, interest coupon, and yield for each separate security; and
3. A statement as to the compliance with this Policy and State law.

### **6.2 ANNUAL REPORTING**

Within 90 days following the end of the fiscal year, the Investment Officers will present to the City Council or the General Government and Finance Advisory Board a comprehensive annual report on the investment program and investment activity. In addition to the information required for quarterly reporting, the annual report will include a review of the activities and return for the twelve months, suggest Policy revisions and improvements that might enhance the investment program, and include an investment plan for the ensuing fiscal year. The annual report may be a component of the quarterly report.

### **6.3 PERFORMANCE STANDARDS**

To evaluate portfolio performance of funds subject to this Policy, the City establishes "weighted average yield to maturity" as the standard portfolio performance measurement. The portfolio's performance will be compared against appropriately competitive and reasonable benchmarks, including money market mutual funds or investment pools of similar make-up and maturities.

### **6.4 COMPLIANCE**



The quarterly reports shall be formally reviewed and a compliance audit of management controls and adherence to this Policy as it relates to the City's investments and investing activity will be performed on an annual basis in conjunction with the City's annual financial audit. The results shall be reported to the City Council.

## **SECTION 7: POLICY REVIEW AND AMENDMENTS**

This Investment Policy will be reviewed by the City Council on at least an annual basis as required by the Public Funds Investment Act. The City Council shall adopt a written instrument by rule, order, ordinance, or resolution stating that it has reviewed the investment policy and investment strategies and the written instrument so adopted shall record any changes made to either the investment policy or investment strategy.

**CITY OF GEORGETOWN INVESTMENT POLICY  
Attachment "A"**

**Approved Broker/Dealer List**

---

FHN Financial

Duncan Williams

Hilltop Securities

Multi-Bank Securities

SAMCO Capital

Rice Financial

Wells Fargo Securities

These broker/dealers meet the City's Investment Policy requirements.

RESOLUTION NO. \_\_\_\_\_

**A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF GEORGETOWN,  
TEXAS, AMENDING THE EXISTING CITY OF GEORGETOWN INVESTMENT  
POLICY EFFECTIVE DECEMBER 8, 2020.**

WHEREAS, the goal of the City of Georgetown is to implement an investment policy that utilizes all current municipal investment practices, while ensuring the safety and availability of all funds entrusted to the City in compliance with federal, state and local laws; and

WHEREAS, the City Council of the City of Georgetown has reviewed the investment policy; and

WHEREAS, the City Council of the City of Georgetown wishes to amend its Investment Policy (as last amended December 10, 2019); and

**NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF  
GEORGETOWN, TEXAS, THAT:**

SECTION 1. The facts and recitations contained in the preamble of this resolution are hereby found and declared to be true and correct, and are incorporated by reference herein and expressly made a part hereof, as if copied verbatim. The enactment of this resolution is not inconsistent or in conflict with any 2030 Plan Policies.

SECTION 2. The Investment Policy attached as Exhibit "A" is hereby adopted by the City Council of the City of Georgetown, Texas.

SECTION 3. This resolution shall be effective immediately upon adoption.

RESOLVED this 8th day of December 2020.

ATTEST:

THE CITY OF GEORGETOWN:

\_\_\_\_\_  
Robyn Densmore  
City Secretary

\_\_\_\_\_  
Dale Ross  
Mayor

APPROVED AS TO FORM:

\_\_\_\_\_  
Skye Masson  
City Attorney

City of Georgetown, Texas  
Government and Finance Advisory Board  
October 28, 2020

**SUBJECT:**

Consideration and possible recommendation to Council of a contract with Suddenlink to provide dedicated Internet service for a total of \$136,620 over three years. - James Davis, IT Manager - Operations

**ITEM SUMMARY:**

This item is to request approval of a new three-year contract with Suddenlink for a dedicated internet circuit for a total of \$136,620 (\$3,795 a month). Suddenlink provides the following services to the City of Georgetown: 1. Primary Internet services delivered over dedicated fiber optic cables. 2. A dedicated fiber line to send the City's Channel 10 video feed to Suddenlink. 3. All public IP addresses that connect City of Georgetown servers to the public Internet. No other vendor can reasonably provide this combination of services to City facilities. This contract reduces the cost of services by \$360 per month while increasing the amount of bandwidth available to the City from 200 megabits/second to 2 gigabytes/second. The cost was reduced by eliminating a redundant fiber path to the City's datacenter. This path was no longer needed as the City recently added a second internet service provider that terminates at the new Disaster Recovery datacenter. The Legal Department has reviewed and approved the attached contract.

**FINANCIAL IMPACT:**

All items were budgeted during the FY 2021 budget process. Expenses will be recorded in CC0652 (IT Management) in spend category (Software Maintenance Subscriptions and Support Services).

**SUBMITTED BY:**

Sharon Parker

**ATTACHMENTS:**

Description	Type
 Suddenlink CSA Rev Final	Backup Material



## Service Agreement/ Order Form

Date: 9/16/2020

### Customer Information

Customer Status: Existing Customer

Customer Name: CITY OF GEORGETOWN IT-Library Internet Services

Billing Address: PO Box 409

*Street Address Suite City State Zip Code*

Billing Contact: Accounts Payable *Phone* 512-930-4357 *Email* itbilling@georgetown.org

Order Contact: James Davis *Phone* 512-930-3656 *Email* james.davis@georgetown.org

Suddenlink Contact: Andrew Hudson *Phone* (903) 714-2125 *Email* andrew.hudson@alticeusa.com

### Suddenlink Services

The above Customer agrees to the ordering of the following Services:

Order Type: Renewal - Service Upgrade  
Service Location Type: LIT  
'A' Location: 510 W 9TH ST, GEORGETOWN, TX 78626  
Demarc: 1st Floor MDF closet

Account #: 7309760011  
Service Location Type:  
'Z' Location:  
Demarc:  
Type II: ☐

	Individual Monthly Recurring Charge	Quantity	Total Monthly Recurring Charge	Non Recurring Charge
1 Optical Internet Access 2G 2Gb	\$3,795.00	1	\$3,795.00	\$0.00
Service Term: 3 years				
Total Monthly Recurring Charge: \$3,795.00				
Total Installation Charge: \$0.00				
For Internal Use Only				

### Remarks

### Terms and Conditions

Ceque Communications, LLC dba Suddenlink Communications ("Suddenlink" or "Altice Business") and Customer acknowledge and agree to be bound by the Terms and Conditions attached hereto. Customer will be responsible for the rates listed on the Service Agreement form and all applicable local, state and federal taxes, charges and assessments along with any other applicable charges. Customers purchasing Suddenlink Business Hosted Voice Service (on Fiber) are also subject to Business Hosted Additional T&C's for Fiber <https://www.suddenlink.com/terms-and-policies> and Exhibits attached hereto and made part of this Agreement

Notice Regarding E911 Services. While your Suddenlink Phone Service may be supported by a battery backup, it is electrically powered. In the event of a power outage or Suddenlink network failure, 911 services will not be available. You are prohibited from moving the phone modem from the address where it was installed. If you move the phone modem, the 911 service may not function properly and emergency operators will not be able to identify the caller's location.

By signing this Agreement; (i) you represent that you are the Customer or Customer's authorized agent; (ii) you agree that you have received a copy of and have been given an opportunity to review this Commercial Service Order and Agreement; (iii) you agree to the terms and conditions of the Commercial Service Agreement; (iv) you acknowledge that you have read and understood the Notice Regarding 911 Services above; This Agreement shall not be deemed effective until it has been executed by both parties.

Agreed by:

Customer

Authorized Signature: \_\_\_\_\_

Print Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

Email: \_\_\_\_\_

Phone: \_\_\_\_\_

Ceque Communications, LLC dba Suddenlink Communications

Authorized Signature: \_\_\_\_\_

Print Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

## Commercial Service Agreement

Customer ("You" or "Customer") agrees to be bound by this Commercial Service Agreement (the "Agreement") with respect to all services ("Service(s)") provided by Suddenlink Communications and its affiliates and subsidiaries authorized to provide the services set forth herein (collectively, "Suddenlink"). The Agreement includes the general terms of service set forth below, as well as the additional commercial terms of service and terms of service applicable to the specific Services and features to which you subscribe or have access, including cable television service ("Video Service"), high speed data service ("High Speed Internet Service"), voice service ("Phone Service" or "Business Hosted Voice Service on FIBER"), support services and mobile apps, as are set forth below or at <https://www.suddenlink.com/terms-and-policies> and may be updated from time to time (collectively, the "Additional Terms of Service"), which are incorporated in this Agreement by reference. You further understand and agree that the Suddenlink Communications Privacy Policy ("Privacy Policy"), which governs the collection, use and disclosure of Customer personal information, is likewise incorporated herein by reference. THIS AGREEMENT CONTAINS A BINDING ARBITRATION AGREEMENT THAT AFFECTS CUSTOMER'S RIGHTS, INCLUDING THE WAIVER OF CLASS ACTIONS AND JURY TRIALS. THE AGREEMENT ALSO CONTAINS PROVISIONS FOR OPTING OUT OF ARBITRATION. PLEASE REVIEW IT CAREFULLY.

### GENERAL TERMS OF SERVICE APPLICABLE TO SERVICE(S):

1. **Services.** Suddenlink shall use reasonable efforts to make the Services available by any requested service date. Suddenlink shall not be liable for any damages whatsoever resulting from delays in meeting any service dates due to delays resulting from construction or for reasons beyond its control. Suddenlink shall provide Customer with the Services and Equipment identified on the commercial service order presented to Customer at time of installation ("Service Order"); provided, however, if Suddenlink determines that Customer's location is not serviceable under Suddenlink's normal installation guidelines, Suddenlink may terminate this Agreement. Suddenlink shall have no responsibility for the maintenance or repair of networks, facilities and equipment not furnished by Suddenlink.
2. **Payment of Charges.** The charges for one month of Services, including any deposits, activation, set-up, installation, construction and/or Equipment charges, are due upon installation of the Services or as otherwise set forth on the Service Order. Thereafter, Customer agrees to pay monthly recurring Service charges and Equipment charges (if any) in advance, including all applicable fees (such as restoration or experience fees), taxes, regulatory fees, franchise fees, surcharges (including sports and broadcast tv surcharges), or other government assessments no later than the date indicated on Customer's bill. Charges for non-recurring Services or Equipment charges will be reflected on Customer's subsequent bill at the then current applicable rates. All rates for Services, Equipment charges and other fees and surcharges are subject to change in accordance with applicable law. If Customer elects to pay by automatic recurring credit card, debit card or automatic clearing house payments, Customer authorizes Suddenlink to charge such accounts. If Customer elects to send a check as payment, Customer authorizes Suddenlink either to use information from Customer's check to make a one-time electronic funds transfer from Customer's bank account or to process the payment as a check transaction. Failure to receive a bill does not release Customer from Customer's obligation to pay. Failure to pay the total balance when due (including checks returned for insufficient funds) shall constitute a breach of this Agreement and may be grounds for termination of Service, removal of Equipment from Customer's premises and/or imposition of a late fee ("Late Fee") in accordance with applicable law. You can avoid incurring Late Fees by paying your monthly bill promptly. Any Late Fee imposed on Customer is intended to be a reasonable advance estimate of costs of managing past due accounts. The Late Fee is not interest, a credit service charge or a finance charge. If the Customer has more than one account (Business and/or Residential) served by Suddenlink, all Suddenlink-provided Services at all locations may be subject to discontinuance of Service in the event any one account remains unpaid. In the event collection activities are required, an additional collection charge may be imposed.
3. **Additional Fees.** In addition to Customer's monthly recurring charges and any Late Fee, additional fees may be imposed, including fees for returned checks, Payment Assistance Fees for paying by phone, receiving a paper bill, charge card chargeback, early termination, reconnection and service calls. Additional charges may also be imposed if collection activities are required to recover past due balances, including attorney fees. A list of applicable fees ("Schedule of Fees") is available at [www.suddenlink.com/pricing-packages](http://www.suddenlink.com/pricing-packages). Suddenlink reserves the right to amend or change the Schedule of Fees from time to time.
4. **Third Party Provider Charges.** In connection with Customer's use of the Services and Equipment, Customer may be able to access, subscribe to, use and/or purchase products, services, software or applications that are provided to Customer by third parties ("Third Party Providers"). Customer acknowledges that Customer may incur charges in connection with the subscription to, purchase or use of these Third-Party Provider products, services, software or applications. All such charges, including any additional fees and applicable taxes, shall be paid by Customer to the Third-Party Provider and are not the responsibility of Suddenlink. Credits or billing adjustments for products, services, software or applications billed by a Third-Party Provider shall be subject to the stated billing practices of that Third-Party Provider. Termination of a service or subscription offered for a separate charge billed directly by a Third-Party Provider shall be effected in accordance with the Terms of Service or similar agreement between the Customer and the Third-Party Provider.
5. **Taxes.** Customer agrees to pay any local, state or federal taxes imposed or levied on or with respect to the Services, the Equipment or installation or service charges incurred with respect to the same.
6. **Term; Early Termination.** Your Service Term subscription begins either on or the first day following your installation date and continues for the initial term set forth on your Service Order ("Initial Term"). If a Service Order does not specify an Initial Term, You have an automatically renewing monthly Term subscription ("Monthly Subscription").
  - a. **Monthly Term.** If you have a Monthly Subscription, your subscription begins either on or the first day following your installation date and automatically renews thereafter on a monthly basis beginning on the first day of the next billing period assigned to you until cancelled by you. The monthly service charge(s) will be billed at the beginning of your assigned billing period and each month thereafter unless and until you cancel your Service(s). PAYMENTS ARE NONREFUNDABLE AND THERE ARE NO REFUNDS OR CREDITS FOR PARTIALLY USED SUBSCRIPTION PERIOD(S). You may cancel Service(s) for a period up to the last day of the billing period prior to the service period that you wish to cancel, and the cancellation will be effective at the end of the then-current billing period. Any request for cancellation after the commencement of a service period will be effective at the end of the then-current service period. Access to the Services will, if possible, continue to be provided at the location ordered or, if you move, to your new location if in an Suddenlink-served area (subject to any installation charges).
  - b. **Initial Term Subscription.** If You have an Initial Term, your subscription begins either on or the first day following your installation date and continues for the duration of the applicable Initial Term. Upon the expiration of the Initial Term, Your subscription automatically renews thereafter on a monthly basis (each, a "Renewal Month") beginning on the first day of the next billing period assigned to you until cancelled by you. The monthly service charge(s) for each month during the Initial Term and any Renewal Months will be billed at the beginning of your assigned billing period and each month thereafter unless and until you cancel your Service(s). PAYMENTS ARE NONREFUNDABLE AND THERE ARE NO REFUNDS OR CREDITS FOR PARTIALLY USED SUBSCRIPTION PERIOD(S).
    - i. Except as provided below. If Customer cancels, terminate or downgrade the Service(s) before the completion of the Initial Term", you agree to pay Suddenlink early cancellation fees in an amount that includes: (i) all non-recurring charges reasonably expended by Suddenlink to establish service to Customer and not remunerated, (ii) any disconnection, early cancellation or termination charges reasonably incurred and paid by Suddenlink to third parties on behalf of Customer, and (iii) all monthly recurring charges for Services and Equipment for the remaining balance of the Initial Term. Notwithstanding the foregoing, this Agreement is subject to the availability of funding. In the event that funds do not become available the Agreement may be terminated or the scope may be amended. A 30-day written notice will be provided to Suddenlink and there will be no penalty nor other charges incurred by the City.
    - ii. Following the Initial Term, You may cancel Service(s) for a period up to the last day of the billing period prior to the service period that you wish to cancel, and the cancellation will be effective at the end of the then-current billing period. Any request for cancellation after the commencement of a service period will be effective at the end of the then-current service period. Access to the Services will, if possible, continue to be provided at the location ordered or, if you move, to your new location if in a Suddenlink-served area (subject to any installation charges).
7. **Right to Make Credit Inquiries.** Customer acknowledges and agrees that Suddenlink may (a) verify Customer's credit standing, make inquiries and receive information about your credit experiences, including your credit report, from credit reporting agencies; (b) enter this information in your file, and disclose this information concerning you to appropriate third parties for reasonable business purposes; and (c) furnish information about you, your account(s) and your payment history to those credit reporting agencies.
8. **Security Deposit.** Suddenlink may require a deposit or activation fee based on Customer's credit standing or past payment history with Suddenlink. A deposit or activation fee does not relieve the Customer of the responsibility for the prompt payment of bills on presentation. Any security deposit given by Customer for the Equipment or Suddenlink's Service will be due and payable upon the first monthly billing. Such security deposits will be returned to Customer within sixty (60) days of termination of Suddenlink's Service so long as payment has been made for all amounts due on Customer's account and Customer has returned the Suddenlink Equipment undamaged. Security deposits paid by Customer for Equipment or Services may be used, to the extent permitted by law, to offset any unpaid balance or charges after termination of Service. Customer shall remain liable for any outstanding balances after the security deposit has been applied. Further terms and conditions of the security deposit may be contained in the deposit receipt given to Customer at the time the security deposit is collected.
9. **Disputed Charges.** Customer agrees to pay all undisputed monthly charges and all applicable fees and taxes as itemized on the Suddenlink monthly bill and notify Suddenlink in writing of disputed items or requests for credit within thirty (30) days of Customer's receipt of the bill for which correction of an error or credit is sought, or longer as provided by applicable law. The date of the dispute shall be the date Suddenlink receives sufficient documentation to enable Suddenlink to investigate the dispute. The date of the resolution is the date Suddenlink completes its investigation and notifies the Customer of the disposition of the dispute.
10. **Adjustments or Refunds.** Any adjustment or refund, given in each case in Suddenlink's sole discretion, will be accomplished by a credit on a subsequent bill for Service, unless otherwise required by applicable law. No credit allowance will be made for interruptions of Service that are: (a) due to the negligence of or noncompliance with the provisions of the Agreement by Customer or any person authorized by customer to use the Service; (b) due to the negligence of any person other than Suddenlink including, but not limited to, the other common carriers connected to the Suddenlink's facilities; (c) due to the failure or malfunction of Customer owned equipment or third party equipment; (d) during any period in which Suddenlink is not given full and free access to its facilities and Equipment for the purpose of investigating and correcting interruptions; (e) during a period in which Customer continues to use the Service on an impaired basis; (f) less than thirty (30) minutes' duration; (g) during any period when the interruption is due to implementation of a Customer order for a change in Service arrangements; or (h) due to circumstances or causes beyond the control of Suddenlink. Unless otherwise provided by applicable law, in the event any amounts owed by Suddenlink to Customer are not claimed by Customer within one year of the date on which the amount became payable to Customer, Customer shall forfeit all rights to the refund and all such amounts shall become the property of Suddenlink.
11. **Equipment and Software.** "Distribution System" shall mean (1) all distribution plant, network facilities and associated electronics and all Equipment installed or provided by Suddenlink or its predecessors which is necessary to distribute Services throughout the premises, but specifically excluding Inside Wiring, and (2) all Equipment furnished by Suddenlink at the premises. Ownership of the Distribution System shall at all times be and remain in Suddenlink and shall be used exclusively by and in connection with Suddenlink operations. Upon termination of this Agreement and if Suddenlink is no longer providing Services to the premises, Suddenlink has the option to remove all or any portion of the Distribution System, provided that any damage to the premises caused by removal of the Distribution System will be repaired by Suddenlink to Customer's reasonable satisfaction. "Equipment" means all equipment, including but not limited to, any cables, wires, amplifiers, cable boxes, access cards, remotes, cable cards, battery backup units, modems, routers, gateways, Altice One and Altice One Mini units distributed to and/or installed for use in the Customer's service location but does not include Inside Wiring. "Inside Wiring" shall mean all wiring on the Customer's side of the demarcation point at Customer's service location, whether installed by Suddenlink or by Customer. The demarcation point shall mean a point at (or about) twelve (12) inches outside of where the cable wire enters the Customer's service location. Inside Wiring shall be Customer property and not Suddenlink Equipment, and repair and maintenance for such Inside Wiring is the responsibility of Customer unless otherwise agreed by Customer and Suddenlink. None of the Equipment shall become a fixture nor shall distribution, installation, and/or use of Equipment, including but not limited to cable boxes and/or set top boxes be deemed a lease of such Equipment. Unless otherwise stated in the Service Order, Customer will acquire no ownership or other interest in the Distribution System, Equipment, network facilities, and software by virtue of payments made pursuant to this Agreement or by the attachment of any portion of the Distribution System, Equipment or network facilities to Customer's premises.

- a. **Misuse of Equipment.** Suddenlink Equipment is intended to service and reside at the specific service location and is not to be removed from the service location where it was installed or used off premises without Suddenlink authorization. Customer agrees that neither Customer nor any other person (except Suddenlink's authorized personnel) will open, alter, misuse, tamper with, service, or make any alterations to any Equipment. Customer will not remove any markings or labels from the Equipment. Customer agrees to safeguard the Equipment from loss or damage of any kind, and (except for any self installation procedures approved by Suddenlink) will not permit anyone other than a Suddenlink authorized representative to perform any work on the Equipment. Any misuse, alteration, tampering, or removal, or the use of Equipment which permits the receipt of Services without authorization or the receipt of Services to an unauthorized number of outlets, or to unauthorized locations constitutes theft of service and is prohibited.
- b. **Return of Equipment.** If Customer's Service is terminated or cancelled (for whatever reason), unless Suddenlink expresses otherwise in writing, Customer agrees that Customer no longer has the right to keep or use the Equipment and Customer must promptly return the Equipment. The Equipment must be returned to Suddenlink in the same condition as when received, ordinary wear and tear excepted. Absent other instructions, if Customer fails to return the Equipment, Customer will pay any expenses Suddenlink incurs in retrieving the Equipment. Failure of Suddenlink to remove the Equipment does not mean that Suddenlink has abandoned the Equipment. Suddenlink may impose a charge for unreturned Equipment to be determined in accordance with Suddenlink's then current schedule of charges for non-returned Equipment and/or continue to charge Customer a monthly Service fee every month until any remaining Equipment is returned, collected by Suddenlink or fully paid for by Customer. Any charge for unreturned Equipment shall be due immediately. Suddenlink retains ownership of all Equipment.
- c. **Damaged or Lost Equipment.** If the Equipment is damaged by Customer, destroyed, lost or stolen while in Customer's possession, Customer is responsible for the cost of repair or replacement of the Equipment.
- d. **Operation of Equipment.** Customer agrees to operate any Equipment in accordance with instructions of Suddenlink or Suddenlink's agent. Failure to do so will relieve the Suddenlink Parties of liability for interruption of Service and may make the Customer responsible for damage to Equipment.
- e. **Tests and Inspections.** Upon reasonable notification to the Customer, and at a reasonable time, Suddenlink may make such tests and inspections as may be necessary to determine that the Customer is complying with the requirements set forth herein.
- f. **Software.** Customer agrees to comply with the terms and conditions of any software license agreement applicable to the software provided or installed by Suddenlink ("Software"). The Software shall be used solely in connection with the Services and Customer will not modify, disassemble, translate or reverse engineer, the Software. All rights title and interest to the Software, including associated intellectual property rights, are and will remain with Suddenlink and Suddenlink's licensors. If Customer's Service is terminated, Customer will promptly return or destroy all Software provided by Suddenlink and any related written materials. Suddenlink will have the right to upgrade, modify and enhance the Equipment and Software from time to time. Customer acknowledges that the Software, and any related written materials, may be subject to applicable export control laws and regulations of the USA. Customer agrees not to export or re-export the Software, directly or indirectly, to any countries that are subject to USA export restrictions.
- g. **Repair.** Suddenlink will repair and/or replace defective Software or Equipment provided such damage was not caused by misuse, neglect or other fault of Customer. Suddenlink assumes no responsibility and shall have no responsibility for the operation, maintenance, condition or repair of any Customer-provided equipment and/or software, including, but not limited to, televisions, computer devices, remote controls or other consumer electronics, including any hardware or third party software, which may be connected to the Services ("Customer Equipment"), except that Suddenlink may automatically push required software or firmware updates directly to Customer Equipment when necessary for the provision of Suddenlink Service(s). Customer is responsible for the repair and maintenance of Customer Equipment. Suddenlink is not responsible or liable for any loss or impairment of Suddenlink's Service due in whole or in part to a malfunction, defect or otherwise caused by Customer Equipment. Suddenlink makes no warranties, with respect to Equipment or Service provided by Suddenlink or with respect to the Equipment's compatibility with any Customer Equipment.
- 12. Prohibitions/Theft of Service.** Customer shall not intercept, receive or assist in the interception or receipt of, resell, distribute or duplicate any Services. In no event shall Customer use the Services and/or Equipment to engage in any illegal or prohibited activity.
- 13. Customer Liability for Users.** Customer is responsible for any access, use or misuse of the Services and/or Equipment that may result from access or use by any other person who has access to Customer's premises, equipment or account. Customer is responsible for ensuring that all persons who use Customer's subscribed to Services ("Users") understand and comply with all terms and conditions applicable to the Services.
- 14. Business Hosted Voice on Fiber:** Customers purchasing Business Hosted Voice on Fiber are also bound by the Additional Terms for Business Hosted Voice Service on Fiber found at [www.suddenlink.com/terms-and-policies](http://www.suddenlink.com/terms-and-policies) ("Terms of Service") and additional T&Cs as applicable.
- a. SOFTPHONES, OFF-SITE PHONES & WIFI CONNECTIVITY:** SUDDENLINK ALLOWS THE ABILITY TO ACCESS THE HOSTED VOICE SERVICE THROUGH SOFTPHONES, OFF-SITE PHONES AND WIFI CONNECTIVITY. IN NO EVENT SHALL SUDDENLINK BE RESPONSIBLE FOR, NOR DOES IT WARRANT THE PERFORMANCE OR INTEROPERABILITY OF THE SERVICE IN CONNECTION WITH ANY SOFTPHONES, OFF-SITE PHONES OR WIRELESS CONNECTIVITY. IT IS CUSTOMER'S SOLE RESPONSIBILITY TO SUPPORT AND TROUBLESHOOT ANY RELATED CONNECTIVITY ISSUES UNDER THIS SECTION. CUSTOMER ACKNOWLEDGES AND UNDERSTANDS THE HOSTED VOICE PRODUCT CHARACTERISTICS AS SET FORTH IN THE OFF-SITE REMOTE PHONE AND SOFTPHONE ACKNOWLEDGEMENT. PHONES NOT PROVIDED BY SUDDENLINK UNDER THIS AGREEMENT ARE NOT PERMITTED NOR SUPPORTED AND USE OF SUCH PHONES WILL RESULT IN TERMINATION OF THIS AGREEMENT.
- b. Emergency Calling Services (E911) for Hosted Voice Service:** Customer is responsible for complying with all applicable emergency calling service laws. E911 procedures and restrictions are set forth in Emergency Calling Services Terms and Conditions as applicable.
- 15. SecureNet and SecureNet Services: Altice Business SecureNet Service / Altice Business SecureNet Plus Service:** Altice Business SecureNet Service/AlticeBusiness SecureNet Plus Service purchased pursuant to this Agreement is a turnkey managed Service solution that bundles Altice Business Internet Service (over fiber), Managed DDoS Protection Service, Managed Security Gateway Service, and for Altice Business SecureNet Plus Service, also includes Managed Security Gateway Service with Unified Thread Management, and is subject to the terms and conditions of this Agreement, including those for Managed DDoS Protection Service and Managed Security Gateway Service as set forth below.
- 16. Managed DDoS Protection Service:** Managed DDoS (Distributed Denial of Service) Protection Service purchased pursuant to this Agreement and offered in conjunction with Altice Business Internet Service (over fiber) only, will monitor, detect and mitigate Altice Business Internet Service inbound traffic against DDoS attacks and provide cleansing up to thirty (30) times the contracted bandwidth. Managed DDoS Protection Service is provisioned over Altice Business Internet Service/traffic only.
- 17. Service Level Agreement:** The Service Level Agreement ("SLA") attached hereto as Exhibit A sets forth Customer's sole remedy for any claim relating to the Service including any failure to meet any guarantee as set forth in the SLA.
- 18. Access to Customer Premises.** Customer grants Suddenlink and its employees, agents, contractors, and representatives all necessary rights of access to enter and within Customer's premises, including access to space for cables, conduits and equipment, the wiring within Customer's premises and Customer's computer(s) and other devices, to install, deliver, connect, inspect, maintain, repair, replace, disconnect, remove or alter any and all facilities, check for signal leakage or install or deliver Equipment and Software provided by Suddenlink. Customer shall cooperate in providing such access upon request of Suddenlink. If Customer is not the owner of the premises, Customer warrants that Customer has obtained the legal authority of the owner to authorize Suddenlink personnel and/or its agents to enter the premises for the purposes described herein. Suddenlink's failure to remove its Equipment shall not be deemed an abandonment thereof. Customer shall provide a secured space with electrical power, climate control and protection against fire, vandalism, and other casualty for Suddenlink's equipment. Customer is responsible for ensuring that Customer's equipment is compatible for the Services selected and with the Suddenlink network.
- 19. Violations of this Agreement.** It shall be a violation of this Agreement for Customer or any User (1) to engage in any conduct prohibited by this Agreement (or by any terms and conditions incorporated herein by reference); or (2) not to engage in conduct required by this Agreement, each case determined in Suddenlink's sole good faith discretion. In addition, whether or not the conduct set forth below is elsewhere prohibited by this Agreement, it shall be a violation of this Agreement if: (a) Customer or any User fails to abide by Suddenlink's rules and regulations or to pay the charges billed; (b) Customer or any User fails to provide and maintain accurate registration information or the information required in the registration process is or becomes incorrect, absent or incomplete; (c) Customer or any User engages in any illegal or prohibited activity in connection with their use of any Service; (d) Customer or any User harasses, threatens or otherwise abuses any Suddenlink employee or agent; (e) Customer or any User refuses to provide Suddenlink with reasonable access to the service location or refuses to allow Suddenlink to diagnose and/or troubleshoot a service issue when such access or customer interaction is necessary in order to provide the appropriate customer support; or (f) The amount of customer and/or technical support required to be provided to Customer or any User is excessive in the sole good faith discretion of Suddenlink.
- 20. Termination.** Suddenlink may terminate this Agreement, disconnect or suspend any or all Services, and remove Equipment at any time, without prior notice, for any reason whatsoever or for no reason, including but not limited to if Customer or any User fails to fully comply with the terms of this Agreement and/or any Suddenlink or authorized Third Party Provider terms of service, agreements or policies incorporated herein by reference. If Suddenlink terminates Service due to a violation of this Agreement or Suddenlink's policies, Customer may be subject to additional fees and charges, including disconnect and termination fees and Suddenlink may also exercise other rights and remedies available under law or in equity. The Agreement is subject to the availability of funding. In the event that funds do not become available the Agreement may be terminated or the scope may be amended. A 30-day written notice will be provided to Suddenlink and there will be no penalty nor other charges incurred by the City.
- 21. Effect of Termination by Suddenlink.** Customer agrees that in the event of termination by Suddenlink: (i) Suddenlink and any Third Party Providers of co-branded services offered as part of or through the high speed internet service shall have no liability to Customer or any User; and (ii) unless expressly prohibited by law, Suddenlink, in its sole good faith discretion, may decline or reject a new application for service or block access to or use of any component of the Services by Customer or any former User. Customer further agrees that upon termination of any Service, Customer will immediately cease use of the Equipment and any Software, and; Customer will pay in full the charges for Customer's use of the Service and the Equipment through the later of: (i) Customer's applicable Service month, or (ii) if applicable, the expiration of any promotional term, or, if applicable, (iii) the date when the associated Equipment or Software has been returned to Suddenlink. Failure of Suddenlink to remove Equipment shall not be deemed an abandonment thereof. Customer shall pay reasonable collection and/or attorney's fees to Suddenlink in the event that Customer shall find it necessary to enforce collection or to preserve and protect its rights under this Agreement.
- 22. Content and Services.** All content, program services, program packages, number of channels, channel allocations, broadcast channels, interactive services, email, data offerings and other services are subject to change in accordance with applicable law.
- 23. Disclaimer.** Suddenlink assumes no liability for any program, services, content or information distributed on or through the Services, Equipment or the cable system, unless locally provided by Suddenlink, and Suddenlink expressly disclaims any responsibility or liability for your use thereof. Further, Suddenlink shall not be responsible for any products, merchandise or prizes promoted or purchased through the use of the Services.

**24. Telephone Communications with You Regarding Your Account or Service.** You agree that Suddenlink and its agents may call or text you at any phone number (landline or wireless) that you provide to us, using an automated dialing system and/or a prerecorded message, for non-promotional service and/or account-related purposes, such as appointment confirmations, service alerts, billing and collection issues or account recovery concerns. You agree to notify us: (1) if any such phone number changes; (2) is no longer active; or (3) is ported from a landline to a wireless phone number. You can manage your contact preferences by logging into your account at <http://www.suddenlink.com>.

**25. No Waiver.** The failure of Suddenlink to enforce this Agreement and any of its components, for whatever reason, shall not constitute a waiver of any right of Suddenlink or the ability to assert or enforce such right at any time in the future.

**26. No Assignment.** This Agreement and the Services and/or Equipment supplied by Suddenlink are not assignable or otherwise transferable by Customer, without specific written authorization from Suddenlink. In Suddenlink's discretion, Suddenlink may assign, in whole or in part, this Agreement, and Service may be provided by one or more legally authorized Suddenlink affiliates.

**27. No Warranty; Limitation of Liability.** Customer expressly agrees that: (a) the Services provided are best efforts services and the Services, Software and Equipment are provided by Suddenlink on an "AS IS" and "AS AVAILABLE" basis without warranties of any kind, either express or implied; (b) Suddenlink, its officers, shareholders, directors, employees, affiliates, vendors, carrier partners, content providers and other persons or entities involved in providing the Services or Equipment (collectively, the "Suddenlink Parties") are not responsible or liable for any loss or impairment of service due in whole or in part to Customer owned- or provided- Equipment; and (c) all use of the Services, Software and Equipment, including that provided by Third Party Providers, as well as the purchase, download or use of any third party service, product, or application provided by or accessed through the Services or Equipment, are provided at Customer's sole risk and Customer assumes total responsibility for Customer's or any User's use of the Services. Without limiting the generality of the foregoing, the Suddenlink Parties make no warranty: (i) that the Services will be uninterrupted or error free or that the Equipment will work as intended; (ii) as to transmission or upstream or downstream speeds of the network; (iii) that the Services, Equipment or Software are compatible with any Customer owned- or provided- Equipment; or (iv) as to the security of Customer's communications via Suddenlink's facilities or Services, or that third parties will not gain unauthorized access to or monitor Customer's communications. Customer has the sole responsibility to secure Customer's communications and the Suddenlink Parties will not be liable for any loss associated with such unauthorized access. In addition, neither the Suddenlink Parties nor any Third Party Provider of services or products makes any representations or warranties with respect to any product or services offered through the Services or Equipment, and Suddenlink shall not be party to nor responsible for monitoring any transaction between Customer and any Third Party Provider of products or services.

Except for a refund or credit as expressly provided in this Agreement, in no event (including negligence) will the Suddenlink Parties be held responsible or liable for any loss, damage, cost or expense including direct, indirect, incidental, special, treble, punitive, exemplary or consequential losses or damages including, but not limited to, loss of profits, earnings, business opportunities, loss of data, personal injury (including death), property damage or legal fees and expenses, sought by Customer or anyone else using Customer's Service account: (x) resulting directly or indirectly out of the use or inability to use the Services (including the inability to access emergency 911 or e911 services) and/or use of the Software, Equipment or provided third party services or otherwise arising in connection with the installation, maintenance, failure, removal or use of Services, Software and/or Equipment or Customer's reliance on the Services, Software and/or Equipment, including without limitation any mistakes, omissions, interruptions, failure or malfunction, deletion or corruption of files, work stoppage, errors, defects, delays in operation, delays in installation, failure to maintain proper standards or operation, failure to exercise reasonable supervision, delays in transmission, breach of warranty or failure of performance of the Services, Software and/or Equipment; or (y) resulting directly or indirectly out of, or otherwise arising in connection with, any allegation, claim, suit or other proceeding relating to Services, Software and/or Equipment, or the infringement of the copyright, patent, trademark, trade secret, confidentiality, privacy, or other intellectual property or contractual rights of any third party. Suddenlink's Maximum Liability to Customer arising under this Agreement shall be the lesser of \$5,000.00 or the amount actually paid by Customer for Services hereunder for the respective regular billing period.

**28. Indemnification. To the extent permitted by law.** Customer agrees to defend, indemnify, and hold harmless Suddenlink Parties from and against any and all claims and expenses, including reasonable attorneys' fees, arising out of or related in any way to the use of the Service and Equipment by Customer or otherwise arising out of or related in any way to the use of Customer's account or any equipment or facilities in connection therewith, or the use of any other products or services provided by Suddenlink to Customer. Customer agrees to indemnify and hold harmless the Suddenlink Parties against claims, losses or suits for injury to or death of any person, or damage to any property which arises from the use, placement or presence or removal of Suddenlink's Equipment, facilities and associated wiring on Customer's premises and further, Customer indemnifies and holds harmless the Suddenlink Parties against claims for libel, slander, or the infringement of copyright arising directly or indirectly from the material transmitted over the facilities of Suddenlink or the use thereof by Customer; against claims for infringement of patents arising from combining with or using in connection with, facilities furnished by Suddenlink, and apparatus, Equipment, and systems provided by Customer; and against all other claims arising out of any act or omission of Customer in connection with the Services or facilities provided by Suddenlink.

**29. Regulatory Authority.** This Agreement and the obligations of the parties shall be subject to modification to comply with all applicable laws, regulations, court rulings, and administrative orders, as amended.

**30. BINDING ARBITRATION. Please read this section carefully. It affects your rights.** Any and all disputes arising between You and Suddenlink, including its respective parents, subsidiaries, affiliates, officers, directors, employees, agents, predecessors, and successors, shall be resolved by binding arbitration on an individual basis in accordance with this arbitration provision. This agreement to arbitrate is intended to be broadly interpreted. It includes, but is not limited to: claims arising out of or relating to any aspect of the relationship between us, whether based in contract, tort, statute, fraud, misrepresentation or any other legal theory; claims that arose before this or any prior Agreement, claims that may arise after the termination of this Agreement. Notwithstanding the foregoing, either You or Suddenlink may bring claims in small claims court in Your jurisdiction, if that court has jurisdiction over the parties and the action and the claim complies with the prohibitions on class, representative, and private attorney general proceedings and non-individualized relief discussed below. You may also bring issues to the attention of federal, state, and local executive or administrative agencies. Resolving Your dispute with Suddenlink through arbitration means You will have a fair hearing before a neutral arbitrator instead of in a court before a judge or jury. YOU AGREE THAT BY ENTERING INTO THIS AGREEMENT, YOU AND SUDDENLINK EACH WAIVE THE RIGHT TO A TRIAL BY JURY AND THE RIGHT TO PARTICIPATE IN A CLASS, REPRESENTATIVE, OR PRIVATE ATTORNEY GENERAL ACTION.

- a. **Opting Out of Arbitration.** IF YOU HAVE BEEN AN EXISTING CUSTOMER FOR AT LEAST 30 DAYS BEFORE THE EFFECTIVE DATE OF THIS AGREEMENT AND HAVE PREVIOUSLY ENTERED INTO AN ARBITRATION AGREEMENT WITH SUDDENLINK OR A PREDECESSOR COMPANY, THIS OPT-OUT PROVISION DOES NOT APPLY TO YOU. IF YOU BECAME A CUSTOMER ON OR WITHIN 30 DAYS OF THE EFFECTIVE DATE OF THIS AGREEMENT, AND DO NOT WISH TO BE BOUND BY THIS ARBITRATION PROVISION, YOU MUST NOTIFY SUDDENLINK IN WRITING WITHIN 30 DAYS OF THE EFFECTIVE DATE OF THIS AGREEMENT BY EMAILING US AT NOARBITRATION@ALTICEUSA.COM OR BY MAIL TO ALTICE SHARED SERVICES, 200 JERICHO QUADRANGLE, JERICHO, NY 11753 ATTN. ARBITRATION. YOUR WRITTEN NOTIFICATION TO SUDDENLINK MUST INCLUDE YOUR NAME, ADDRESS, AND SUDDENLINK ACCOUNT NUMBER AS WELL AS A CLEAR STATEMENT THAT YOU DO NOT WISH TO RESOLVE DISPUTES WITH SUDDENLINK THROUGH ARBITRATION. YOUR DECISION TO OPT OUT OF THIS ARBITRATION PROVISION WILL HAVE NO ADVERSE EFFECT ON YOUR RELATIONSHIP WITH SUDDENLINK OR THE DELIVERY OF SUDDENLINK SERVICES TO YOU. OPTING OUT OF THIS ARBITRATION PROVISION HAS NO EFFECT ON ANY OTHER OR FUTURE ARBITRATION AGREEMENTS THAT YOU MAY HAVE WITH SUDDENLINK.
- b. **Pre-Arbitration Process.** (i) **Notice Of Dispute.** Before commencing an action in arbitration, You must first notify us of Your dispute and allow us an opportunity to resolve it without the need for arbitration. You must write us a letter briefly explaining the dispute and stating the relief that You demand. Provide as much information as possible, including where applicable dates and specific amounts of money. Also include the account holder's name, the account number, the service address, and a telephone number at which You may be reached during business hours. For Your convenience, You may download a Notice of Dispute form from our website at <https://www.suddenlink.com/sites/default/files/Notice-Of-Dispute.pdf>. Once you have written the letter or filled out the Notice, send it to us by certified mail at Altice Shared Services, 200 Jericho Quadrangle, Jericho, NY 11753, Attn: Customer Disputes. (ii) **30 Day Wait Period.** If Suddenlink has not been able to resolve your dispute to your satisfaction within 30 days from when we received your Notice of Dispute, you may start arbitration proceedings.
- c. **Commencing an Arbitration.** To commence an arbitration, you must submit a written Demand for Arbitration to the American Arbitration Association ("AAA"), Case Filing Services, 1101 Laurel Oak Road, Suite 100, Voorhees, NJ 08043, with a copy to Suddenlink. A Demand for Arbitration form can be found on the AAA website at <https://www.adr.org/CommercialForms>.
- d. **Arbitration Process.** The arbitration will be administered by the AAA under the AAA's Commercial Arbitration Rules, as modified by this arbitration provision. You may obtain copies of those rules from the AAA at [www.adr.org](http://www.adr.org). If the AAA will not enforce this arbitration provision as written, it cannot serve as the arbitration organization to resolve Your dispute. If this situation arises, or if the AAA for any reason cannot serve as the arbitration organization, the parties shall agree on a substitute arbitration organization or ad hoc arbitration, which will enforce this arbitration provision as to the dispute. If the parties are unable to agree, the parties shall mutually petition a court of appropriate jurisdiction to appoint an arbitration organization or ad hoc arbitrator that will administer arbitration under this arbitration provision as written. If there is a conflict between this arbitration provision and the AAA rules, this arbitration provision shall govern. A single arbitrator will resolve the dispute between You and Suddenlink. Participation in arbitration may result in limited discovery. The arbitrator will honor claims of privilege recognized by law and will take reasonable steps to protect confidential or proprietary information, including customer personally identifiable information. All issues are for the arbitrator to decide, except that issues relating to arbitrability, the scope or enforceability of this arbitration provision, or the interpretation of its prohibitions of class, representative, and private attorney general proceedings and non-individualized relief shall be for a court of competent jurisdiction to decide. The Arbitrator is limited and bound by terms of this arbitration provision. Although the arbitrator shall be bound by rulings in prior arbitrations involving the same customer to the extent required by applicable law, the arbitrator shall not be bound by rulings in other arbitrations involving different customers. The arbitrator will make any award in writing but need not provide a statement of reasons unless requested by a party. An award rendered by the arbitrator may be entered in any court having jurisdiction over the parties for purposes of enforcement. Unless the parties agree otherwise, any arbitration hearing will take place in the county (or parish) of Your service address. If the amount in dispute is less than \$50,000, Suddenlink agrees that You may choose whether the arbitration is conducted solely on the basis of documents submitted to the arbitrator, by a telephonic hearing, or by an in-person hearing as established by AAA rules. If the amount in dispute exceeds \$75,000 or the claim seeks any form of injunctive relief, either party may appeal the award to a three-arbitrator panel administered by AAA by a written notice of appeal within thirty (30) days from the date of entry of the written arbitration award. An award of injunctive relief shall be stayed during any such appeal. The members of the three-arbitrator panel will be selected according to AAA rules. The three-arbitrator panel will issue its decision within one hundred and twenty (120) days of the date of the appealing party's notice of appeal. The decision of the three-arbitrator panel shall be final and binding, subject to any right of judicial review that exists under the FAA.
- e. **Arbitration Fees.** Except as otherwise provided in this arbitration provision, Suddenlink will pay all arbitration filing, administrative, and arbitrator fees for any arbitration that Suddenlink commences or that You commence seeking damages of \$10,000 or less. If You commence an arbitration seeking greater than \$10,000 in damages, arbitration filing, administrative, and arbitrator fees shall be allocated in accordance with the AAA rules. If You cannot pay Your share of these fees, You may request a fee waiver from the AAA. In addition, Suddenlink will consider reimbursing Your share of these fees if You indicate You cannot afford them and, if appropriate, will pay directly all such fees upon Your written request prior to the commencement of the arbitration. You are responsible for all additional costs and expenses that You incur in the



arbitration, including, but not limited to, attorneys' or expert witness fees and expenses, unless the arbitrator determines that applicable law requires Suddenlink to pay those costs and expenses. Notwithstanding the foregoing, if the arbitrator concludes that Your claim is frivolous or has been brought for an improper purpose (as measured by the standards of Federal Rule of Civil Procedure 11(b)), then the AAA rules shall govern the allocation of arbitration fees, and You agree to reimburse Suddenlink for any amounts Suddenlink may have paid on Your behalf.

- f. **Governing Law.** Because the Service(s) provided to You involves interstate commerce, the Federal Arbitration Act ("FAA"), not state arbitration law, shall govern the arbitrability of all disputes under this arbitration provision. Any state statutes pertaining to arbitration shall not be applicable.
- g. **Waiver of Class and Representative Actions.** YOU AGREE TO ARBITRATE YOUR DISPUTE AND TO DO SO ON AN INDIVIDUAL BASIS; CLASS, REPRESENTATIVE, AND PRIVATE ATTORNEY GENERAL ARBITRATIONS AND ACTIONS ARE NOT PERMITTED. You and Suddenlink agree that each party may bring claims against the other only in Your or its individual capacity and may not participate as a class member or serve as a named plaintiff in any purported class, representative, or private attorney general proceeding. This arbitration provision does not permit and explicitly prohibits the arbitration of consolidated, class, or representative disputes of any form. In addition, although the arbitrator may award any relief that a court could award that is individualized to the claimant and would not affect other Suddenlink account holders, neither You nor Suddenlink may seek, nor may the arbitrator award, non-individualized relief that would affect other account holders. Further, the arbitrator may not consolidate or join more than one person's claims unless all parties affirmatively agree in writing. If any of the prohibitions in the preceding paragraph is held to be unenforceable as to a particular claim, then that claim (and only that claim) must be severed from the arbitration and brought in court. In that instance, or any instance when a claim between You and Suddenlink proceeds to court rather than through arbitration, You and Suddenlink each waive the right to any trial by jury through this Agreement.
- h. **Severability and Survival.** If any other portion of this arbitration provision is determined to be unenforceable, then the remainder of this arbitration provision shall be given full force and effect. The terms of the arbitration provision shall survive termination, amendment or expiration of this Agreement.
- 31. Governing Law.** Subject to Section 26.f above, this Agreement shall be governed by the laws of the state of TEXAS.
- 32. Severability.** If any term or condition of this Agreement shall be adjudicated or determined as invalid or unenforceable by a court, tribunal or arbitrator with appropriate jurisdiction over the subject matter, the remainder of the Agreement with respect to such claim shall not be affected and shall remain valid and enforceable to the fullest extent permitted by law.
- 33. No Relationship.** Nothing in this Agreement will create any joint venture, joint employer, franchisee-franchisor, employer-employee or principal-agent relationship between Suddenlink and any content, backbone, network, circuit and other technology or communications providers, software and other licensors, hardware and equipment suppliers or other third party providers of elements of the High Speed Internet Service, nor impose upon any such companies any obligations for any losses, debts or other obligations incurred by the other.
- 34. Survival.** All representations, warranties, indemnifications, dispute resolution provisions and limitations of liability contained in this Agreement shall survive the termination of this Agreement, as well as any other obligations of the parties hereunder which, by their terms, would be expected to survive such termination or which relate to the period prior to termination (including legal conditions, payment, and Suddenlink rights and the rights of others).
- 35. Force Majeure.** Suddenlink Parties shall not be liable for any delay or failure of performance or Equipment due to causes beyond its control, including but not limited to: acts of God, fire, flood, explosion or other catastrophes; any law, order, regulation, direction, action or request of the United States government or of any other government including state and local governments having or claiming jurisdiction over Suddenlink, or of any department, agency, commission, bureau, corporation or other instrumentality of any one or more of these federal, state, or local governments or of any military authority; preemption of existing service in compliance with national emergencies, acts of terrorism, insurrections, riots, wars, unavailability of rights-of-way, material shortages, strikes, lockouts, or work stoppages.
- 36. Entire Agreement.** This Agreement, including the applicable Additional Terms of Service, Privacy Policy and Acceptable Use Policy ("AUP"), the Service Order and the Schedule of Fees constitute the entire agreement between Suddenlink and Customer with respect to the Services. No undertaking, representation or warranty made by an agent or representative of Suddenlink in connection with the sale, installation, maintenance or removal of Suddenlink's Services or Equipment shall be binding on Suddenlink except as expressly included herein.
- 37. Amendment; Notice.** Suddenlink may, in its sole discretion, change, modify, add or remove portions of this Agreement at any time. Suddenlink may notify Customer of any such changes to this Agreement, or any other required or desired notice hereunder, by posting notice of such changes on Suddenlink's website ([www.suddenlink.com](http://www.suddenlink.com)), or by sending notice via email or postal mail to Customer's billing address, and/or by contacting the telephone number(s) on Customer's account (including mobile phones) by means such as but not limited to browser bulletins, walled garden (browser interruption), voice, SMS, MMS, and text messages, including by the use of by automatic telephone dialing systems. Customer agrees that any one of the foregoing will constitute sufficient notice. Because Suddenlink may from time to time notify Customer about important information regarding the Services, the Privacy Policy and this Agreement by such methods, Customer agrees to regularly check postal mail, e-mail and all postings on the Suddenlink web site ([www.suddenlink.com](http://www.suddenlink.com)) and Customer bears the risk of failing to do so. The Customer's continued use of the applicable Service(s) following notice of such change, modification or amendment shall be deemed to be the Customer's acceptance of any such revision. If Customer does not agree to any revision of this Agreement, Customer must immediately cease use of the all Service(s) and notify Suddenlink that Customer is cancelling this Agreement in accordance with the then-current policy. Customer shall not be responsible for any termination fees if the Agreement is cancelled due to Suddenlink's modification of this Agreement or its Services

## Service Level Agreement - Fiber Services Only (non-coax)

This Service Level Agreement ("SLA") covers the local transport area to the Suddenlink demarcation point including Suddenlink equipment associated with the endpoints such as POE devices and routers. The provisions described below shall be Customer's sole and exclusive remedy in the event of Interruption.

### **MEAN TIME TO REPAIR**

Suddenlink's objective is a four (4) hour mean-time-to-repair ("MTTR")

### **SERVICE LEVEL GUARANTEE**

**Interruption/Outage ("Interruption"):** Defined as a total loss of Service.

**Service Level Guarantee:** If Customer detects an Interruption, Customer shall open a trouble ticket with Suddenlink Network Operation Center by calling 866-232-5455 (option 4) or via the customer portal at Suddenlink.com. An Interruption period begins when Customer reports a circuit/service failure, opens a valid trouble ticket and releases it for testing and repair. The controlling record for the purpose of determining the duration of the Interruption and calculating credits shall be the date/time stamp on the trouble reporting ticket as generated by Altice Business's trouble reporting system. An Interruption period ends when the circuit/service is operative.

- a. If Customer reports a circuit/service to be inoperative but declines to release it for testing and repair, it is considered to be impaired, but not Interrupted.
- b. If an Altice Business technician is dispatched for a reported failure and it is determined that such failure is not within Altice Business's control, Customer will be subject to a truck roll fee for any subsequent dispatch/truck roll(s) requested.
- c. Customer may request a credit, in writing, and reference the date of the ticket. Requests for credit must be submitted to customercare@suddenlink.com within thirty (30) calendar days of the Interruption.
- d. For calculating credit allowances, every month is considered to have thirty (30) days.
- e. A credit allowance is applied on a pro rata basis against the monthly recurring charge for the affected circuit/service and is dependent upon the length of the Interruption.

Altice Business shall credit Customer's monthly recurring charges for the circuit/service experiencing the Interruption as follows:

<b><u>Outage Duration</u></b>	<b><u>Credit of Monthly Charges</u></b>
Less than 30 minutes	none
30 minutes up to but not including 3 hrs	1/10 of a day
3 hrs up to but not including 6 hrs	1/5 of a day
6 hrs up to but not including 9 hrs	2/5 of a day
9 hrs up to but not including 12 hrs	3/5 of a day
12 hrs up to but not including 15 hrs	4/5 of a day
15 hrs up to and including 24 hrs	1 day
Over 24 hours	2 days for each full 24-hour period

**Limitations:** Total credits in a given month shall not exceed one hundred percent (100%) of the monthly recurring charge for the affected circuit/service in that month.

**Chronic Interruption:** Defined as three (3) separate Interruptions of two (2) hours or more on the same facility, within a consecutive thirty (30) day period and/or an Interruption that lasts longer than forty-eight (48) hours. In the event Customer experiences Chronic Interruptions in Service, Altice Business will perform a detailed investigation, report the findings to Customer and, if necessary, institute a corrective plan. If Customer experiences any additional Interruptions on the circuit and a plan for corrective action has been implemented for thirty (30) days, Customer may terminate the affected circuit/service without any further liability upon thirty (30) days prior written notice.

### **No credit allowance will be made for:**

- a. Interruptions caused by the negligence of Customer or third parties outside of Altice Business's control.
- b. Interruptions due to the failure of power, equipment, systems or connections not provided by Altice Business under this Agreement.
- c. Interruptions during any period when Customer has released the circuit for maintenance or rearrangement purposes or for the implementation of a Customer order.
- d. Interruptions which continue because of Customer's failure to authorize replacement of any element of the Service.
- e. Interruptions due to force majeure events.
- f. No trouble found or where the fault of the trouble is undetermined.

City of Georgetown, Texas  
Government and Finance Advisory Board  
October 28, 2020

**SUBJECT:**

Consideration and possible action to recommend to Council the purchase of vehicles and equipment in the amount of \$2,317,620 - Stan Hohman, Fleet Services Manager

**ITEM SUMMARY:**

These vehicles will be purchased through cooperative purchasing agreements. They have been included in the 2020/21 Annual Budget as being either replacement of existing vehicles within the Fleet or as new additions. There are two vehicles being replaced due to hail damage and one wrecked vehicle that was not budgeted. The vehicles and equipment to be purchased in this item include: 3 Small Hybrid SUV's 1 Small Hybrid Sedan 2 Small Mini-Vans 7 Pickups 5 Utility Bed Trucks 3 Utility Mini-Van's 1 Fifteen Passenger Van 1 Flatbed Utility Truck 1 Dump Bed Utility Truck 1 Dump Truck 1 Chipper Bed Truck 1 Electric Bucket Truck 1 Unmarked Police Pickup 2 Unmarked Police Utility Vehicles 2 Unmarked Police Utility Traffic Units 3 Marked Police Utility Traffic Units 9 Marked Police Utility Vehicles In the Fleet Internal Service Fund, departments are charged annual fleet lease fees that are figured by dividing the total purchase cost of the unit by its estimated useful life. These fees are transferred into the fund to pay for replacements. Replacement criteria is based on the unit reaching 100,000 miles or 10 years of service. Considerations given on replacements are the type of service of the unit, how many miles are driven annually, and the reliability of the unit since it has been in service. Out of the 44 units requesting purchase approval, 36 of these are replacements and 8 are new additions approved by Council in the adoption of the FY2021 budget.

**FINANCIAL IMPACT:**

These vehicles were budgeted for in the 2020/21 Fleet Budget. Two vehicles that were hail damaged and the wrecked vehicle that was not budgeted are being paid for with insurance proceeds.

Fund Impacts:

Fleet Replacement ISF	\$819,627.87
Public Safety	\$974,652.49
Electric	\$303,235.50
Insurance/hail	\$127,002.01
Streets	\$93,102.00

**SUBMITTED BY:**

Sharon A Parker

**ATTACHMENTS:**

Description	Type
❑ Cover sheet for Vehicle Purchase	Cover Memo
❑ Vehicles and Equipment FY2021 Summary	Backup Material

# General Government & Finance Advisory Board

(GGAF) Meeting Date: October 28, 2020

Item No.

## AGENDA ITEM COVER SHEET

### SUBJECT

Consideration and possible action to recommend to Council the purchase of vehicles and equipment in the amount of \$2,317,620.

### ITEM SUMMARY

These vehicles will be purchased through cooperative purchasing agreements. They have been included in the 2020/21 Annual Budget as being either replacement of existing vehicles within the Fleet or as new additions. There are two vehicles being replaced due to hail damage and one wrecked vehicle that was not budgeted.

The vehicles and equipment to be purchased in this item include:

- 3 Small Hybrid SUV's
- 1 Small Hybrid Sedan
- 2 Small Mini-Vans
- 7 Pickups
- 5 Utility Bed Trucks
- 3 Utility Mini-Van's
- 1 Fifteen Passenger Van
- 1 Flatbed Utility Truck
- 1 Dump Bed Utility Truck
- 1 Dump Truck
- 1 Chipper Bed Truck
- 1 Electric Bucket Truck
- 1 Unmarked Police Pickup
- 2 Unmarked Police Utility Vehicles
- 2 Unmarked Police Utility Traffic Units
- 3 Marked Police Utility Traffic Units
- 9 Marked Police Utility Vehicles

In the Fleet Internal Service Fund, departments are charged annual fleet lease fees that are figured by dividing the total purchase cost of the unit by its estimated useful life. These fees are transferred into the fund to pay for replacements. Replacement criteria is based on the unit reaching 100,000 miles or 10 years of service. Considerations given on replacements are the type of service of the unit, how many miles are driven annually, and the reliability of the unit since it has been in service.

Out of the **44** units requesting purchase approval, **36** of these are replacements and **8** are new additions approved by Council in the adoption of the FY2021 budget.

### FINANCIAL IMPACT

These vehicles were budgeted for in the 2020/21 Fleet Budget. Two vehicles that were hail damaged and the wrecked vehicle that was not budgeted are being paid for with insurance proceeds.

Fund Impacts:

Fleet Replacement ISF	\$819,627.87
Public Safety	\$974,652.49
Electric	\$303,235.50
Insurance/hail	\$127,002.01
Streets	\$93,102.00

---

**ATTACHMENTS**

Vehicles and Equipment FY2021 Summary

---

Submitted By:

Stan Hohman, Fleet Services Manager

**2021 Vehicle/Equipment Purchase**

Vendor	Description	Unit Replacing	Department	Purchasing Contract	Budgeted	Price	Fund	Disposition
<b>Silsbee Ford</b>	Ford Escape Hybrid AWD	204-02	Airport	GoodBuy Fee	\$35,000.00	\$25,993.96 \$300.00	Fleet ISF	Auction \$1,500
<b>Silsbee Ford</b>	Ford Escape Hybrid	135-09	Engineering	GoodBuy	\$33,500.00	\$27,423.96	Fleet ISF	Auction \$1,500
<b>Cowboy Dodge</b>	Dodge Grand Caravan	Additional	Communications	GoodBuy Fee	\$33,500.00	\$23,912.00 \$300.00	Fleet ISF	Additional
<b>Cowboy Dodge</b>	Dodge Grand Caravan	340-03	Planning	GoodBuy	\$30,000.00	\$23,912.00	Fleet ISF	Pool
<b>Silsbee Ford</b>	Half ton, extended cab, short bed pick up w/tool box	115-15	SCADA	GoodBuy	\$30,000.00	\$26,835.50	Electric	Auction \$2,000
<b>Silsbee Ford</b>	Half ton, extended cab, short bed pick up w/tool box	108-26	Water Plants	GoodBuy	\$30,000.00	\$26,835.50	Fleet ISF	Auction \$1,500
<b>Silsbee Ford</b>	Half ton, extended cab, 4WD, short bed pick up w/tool box	Additional	Engineering	GoodBuy	\$35,000.00	\$29,330.50	Fleet ISF	Additional
<b>Silsbee Ford</b>	Half ton, 4 door, short bed, 4WD	135-04	Engineering	GoodBuy	\$35,000.00	\$32,111.50	Fleet ISF	Auction \$2,000
<b>Silsbee Ford</b>	Half ton, 4 door, short bed, 4WD	Additional	Stormwater	GoodBuy	\$35,000.00	\$32,111.50	Fleet ISF	Additional
<b>Silsbee Ford</b>	One ton, diesel, 4 door, flatbed truck	134-01	Streets	GoodBuy	\$60,000.00	\$49,408.80	Fleet ISF	Auction \$2,500
<b>Silsbee Ford</b>	Three quarter ton, regular cab, long bed pickup	266-03	Animal Control	GoodBuy	\$35,000.00	\$27,187.75	Fleet ISF	Auction \$2,000
<b>Silsbee Ford</b>	Three quarter ton, regular cab, long bed pickup	439-08	Fleet Services	GoodBuy	\$35,000.00	\$27,187.75	Fleet ISF	Pool
<b>Silsbee Ford</b>	Three quarter ton, regular cab, utility truck with overhead rack	435-04	Facilities	GoodBuy	\$45,000.00	\$40,807.60	Fleet ISF	Auction \$2,500
<b>Silsbee Ford</b>	Ford Transit Connect minivan	115-18	Metering Services	GoodBuy	\$30,000.00	\$24,142.00	Electric	Auction \$2,500
<b>Silsbee Ford</b>	Ford Transit Connect minivan	115-49	Metering Services	GoodBuy	\$30,000.00	\$24,142.00	Electric	Auction \$2,500
<b>Silsbee Ford</b>	Ford Transit Connect minivan	115-50	Metering Services	GoodBuy	\$30,000.00	\$24,142.00	Electric	Auction \$1,500
<b>Silsbee Ford</b>	Ford Transit 15 passeger van	Additional	Fleet Services	GoodBuy	\$38,000.00	\$34,184.75	Fleet ISF	Additional
<b>Silsbee Toyota</b>	Toyota RAV4 Hybrid	602-08	Mail Services	GoodBuy Fee	\$33,500.00	\$28,451.00 \$300.00	Fleet ISF	Auction/Pool
<b>Silsbee Ford</b>	One ton, diesel, regular cab, truck w/dump bed	108-22	Water	GoodBuy	\$65,000.00	\$39,972.75	Fleet ISF	Pool
<b>Silsbee Ford</b>	One ton, 4WD, regular cab, utility bed with crane	108-34	Water	GoodBuy	\$65,000.00	\$65,325.15	Fleet ISF	Auction \$2,500
<b>Silsbee Ford</b>	One ton, 4WD, regular cab, utility bed with crane	108-35	Water	GoodBuy	\$65,000.00	\$65,325.15	Fleet ISF	Auction \$2,500
<b>Silsbee Ford</b>	Ford F-550, diesel, regular cab, utility truck body with 7500 lb. capacity Crane	110-33	Water	GoodBuy	\$145,000.00	\$111,126.25	Fleet ISF	Auction \$2,500
<b>Freightliner of Austin</b>	Freightliner M2-106 Single axle, 6 yard dump truck	134-43	Streets	TIPS	\$100,000.00	\$93,102.00	Streets	Auction \$3,500
<b>Altec</b>	Electric Bucket Truck Altec AM-55E	106-48	Electric	Sourcewell	\$240,000.00	\$203,974.00	Electric	Totaled
<b>Freightliner of Austin</b>	Freightliner M2-106 Single axle, with 16 foot chipper body	114-21	Stormwater	TIPS	\$125,000.00	\$108,120.00	Fleet ISF	Auction \$2,500

Vendor	Description	Unit Replacing	Department	Purchasing Contract	Budgeted	Price	Fund	Disposition
Silsbee Ford	Totaled One ton, ext. cab, electric utility bed 4WD	106-65	Electric	GoodBuy	\$0.00	\$56,682.60	Insurance	Totaled
Silsbee Toyota	Hail damaged Toyota Camry Hybrid	925-07	IT	GoodBuy	\$0.00	\$28,073.00	Insurance	Hail Damaged/Totaled
Silsbee Ford	Hail damaged Police Interceptor utility undercover vehicles	864-143	Police	GoodBuy	\$0.00	\$42,246.41	Insurance	Hail Damaged/Totaled
Silsbee Ford	Police Interceptor utility undercover vehicles	864-125	Police	GoodBuy	\$50,000.00	\$42,246.41	Public Safety	Auction/Pool
Lake Country Chevrolet	Half ton, 4 door, short bed pickup	864-130	Police	GoodBuy Fee	\$50,000.00	\$39,320.48 \$300.00	Public Safety	Auction/Pool
Silsbee Ford	Police Interceptor Utility undercover vehicle (Silver)	864-48	Police	GoodBuy	\$70,000.00	\$53,098.42	Public Safety	Auction/Pool
Silsbee Ford	Police Interceptor Utility Silver Traffic Special Unit	864-87	Police	GoodBuy	\$70,000.00	\$55,636.88	Public Safety	Auction/Pool
Silsbee Ford	Police Interceptor Utility Silver Traffic Units (3 Each)	864-84 864-85 864-86	Police	GoodBuy	\$70,000.00 \$70,000.00 \$70,000.00	\$63,780.27 \$63,780.27 \$63,780.27	Public Safety Public Safety Public Safety	Auction/Pool Auction/Pool Auction/Pool
Silsbee Ford	Police Interceptor Utility marked vehicles (9 Each)	864-12 864-24 864-32 864-37 864-43 864-49 864-64 Additional Additional	Police	GoodBuy	\$70,000.00 \$70,000.00 \$70,000.00 \$70,000.00 \$70,000.00 \$70,000.00 \$70,000.00 \$70,000.00 \$70,000.00	\$65,856.61 \$65,856.61 \$65,856.61 \$65,856.61 \$65,856.61 \$65,856.61 \$65,856.61 \$65,856.61 \$65,856.61	Public Safety Public Safety Public Safety Public Safety Public Safety Public Safety Public Safety Public Safety Public Safety	Auction/Pool Auction/Pool Auction/Pool Auction/Pool Auction/Pool Auction/Pool Auction/Pool Additional Additional

ON THIS SHEET			
	Budgeted	Cost	Difference
Fleet ISF	\$978,500.00	\$819,627.87	\$158,872.13
Public Safety	\$1,080,000.00	\$974,652.49	\$105,347.51
Electric	\$360,000.00	\$303,235.50	\$56,764.50
Insurance	\$0.00	\$127,002.01	-\$127,002.01
Streets	\$100,000.00	\$93,102.00	\$6,898.00
<b>Totals</b>	<b>\$2,518,500.00</b>	<b>\$2,317,619.87</b>	<b>\$200,880.13</b>