

COA/CTM DATA CENTER FACILITIES RISK ASSESSMENT

TABLE OF CONTENTS

Author:

Tyler Evans
IT Project Manager

1. INTRODUCTION

- A. Purpose
- B. Business Objective
- C. Scope

2. BACKGROUND

- A. COA/CTM – IT Environment
- B. COA/CTM – Data Center Criticality
- C. Business Risks
- D. COA/CTM Preliminary Assessment

3. EXISTING DATA CENTER’S SPECIFICATIONS

- A. Waller Creek Data Center
- B. City Hall Data Center

4. THE COA VISION AND STRATEGY FOR TARGET STATE

- A. Target State & Risk Benchmark

5. SCOPE OF WORK & ASSOCIATED DELIVERABLES

- A. Data Center Facility Target State “Tier” Development
- B. Data Center Facility Risk Assessment Report
- C. Qualified Recommendations

6. CONSULTANT RESPONSIBILITIES

7. COA RESPONSIBILITIES

8. CONSULTANT RESPONSE REQUIREMENTS

9. PROPOSAL FORMAT, EVALUATION FACTORS, AND OTHER MANDATORY REQUIREMENTS

1. INTRODUCTION

A. Purpose

The purpose of this RFP is for the City of Austin – Communications & Technology Management Division (COA/CTM hereafter) to enter into a fixed contract with a consultant for Data Center Facility Risk Assessment Services (Risk Assessment hereafter). This RFP is standalone initiative – independent of potential future actions related to the COA/CTM's data center assets. The scope of this engagement shall cover two (2) COA/CTM owned & operated data center facilities. Based on budgetary concerns, the Scope of Work & Associated Deliverables (Section #5) should be priced independently for each site.

B. Business Objective

The objective of the Risk Assessment is to assess and document the current COA/CTM owned/operated data center facilities for operational risks, benchmark these facilities against industry standards for organizations of COA/CTM's size & scope, and to develop recommendations for realizing the desired future state of data center facility reliability and lifecycle duration. COA/CTM relies on IT resources to function, so subsequently the 24x7 operation of COA/CTM data centers is essential to the broadest range of COA core mission functions. As such, COA/CTM cannot afford to house its mission critical IT operations in data center facilities which exhibit high inherent risk profiles, subpar facility availability architectures, or short duration lifecycles. COA/CTM requires a baseline of where our mission critical facilities stand in the industry, a high level assessment of the risks we face operating these facilities “as-is”, and options for a cost estimation path to improving overall availability, extending data center facility lifecycles, or potentially sourcing data center facilities from a third party provider - if that proves to be the most viable option.

C. Scope

The chief focus of this assessment shall be based on the primary determinant of availability; the mission critical facilities support systems which enable 24x7X365 data center operations.

In Scope:

- 1) Mission Critical Power Architecture
- 2) Mission Essential HVAC Systems
- 3) Location
- 4) Data Center Environmental, Power, & Operations Monitoring Systems
- 5) Fire Alarm and Suppression Systems

Out of Scope:

- 1) IT Systems (e.g. servers, storage, etc.)
- 2) IT Architecture
- 3) Networking Structures & Telephony

- 4) Outside Plant Fiber Optics
- 6) Logical Security
- 7) Structural Engineering
- 5) Finance
- 6) Physical Security
- 7) Data Cabling
- 8) Growth Capacity
- 9) Data Center Staffing (as it relates to availability risks)
- 10) Data Center Operations
- 11) Energy Efficiency Assessment

2. BACKGROUND

A. COA/CTM - IT Environment

The purpose of this section is to provide an overview of the COA/CTM IT Environment.

The City of Austin is the 14th largest metropolitan area in the United States with over 1.5 million in the MSA and City population of 800,000. It is among the fastest growing cities in the nation. The City's mission is "to be the best managed municipal government in the nation". Governed by a Council-Manager form of government, the Mayor and six member Council, elected at large, appoint the City Manager, who serves as the Chief Administrator of the City organization. The City of Austin consists of over 30 departments, with nearly 12,000 employees ranging widely from hourly employees to degreed professionals, blue collar, and white collar, unionized/non-unionized and sworn public safety officers.

The City of Austin's IT organization has over 500 FTEs, 287 of which are centralized, and an annual budget over \$60 million providing services to City employees and citizens. The central IT department, Communications and Technology Management (CTM), maintains most of the IT infrastructure backbone and provides direct support services to most General Fund departments. Services CTM provides include service desk; support for desktop, applications, network, infrastructure, security and project management office.

A number of IT business units exist to serve the specific departments including:

- Austin Water
- Austin Convention Center
- Aviation
- Austin Library
- Health and Human Services
- Human Resources
- Financial Administrative Services
 - Controller's Office
 - Purchasing Office
 - Budget Office

B. COA-CTM Data Center Criticality

The purpose of this section is to provide some perspective as to the criticality of COA/CTM data center facilities.

Today, the COA cannot operate for long without access to critical IT services and applications. As a result, business risks that impact IT directly and IT risks themselves must now be considered and treated like any significant business risk. Managing in this demanding environment has forced COA to become less tolerant of interruptions that once were acceptable. Data Center facility availability represents the highest common denominator of all IT services rendered, and as such, represents the greatest risk to continuity of service. At current, the vast majority of COA/CTM's IT services are housed & provided for within the Waller Creek Data Center – the primary data center facility. The City Hall Data Center serves as a backup data center facility, but currently holds very limited capacity to restore IT services should the Waller Creek Data Center be offline for any reason. Given this lack of recoverability and redundancy from the IT architectural perspective, the importance and mitigation of operational risk for the data center facilities' themselves takes on an even greater level of importance.

C. Business risks of system downtime include:

All business interruptions cost money. When a critical system is interrupted, the cost of an IT outage can mount fast. The loss of a critical system for even a few hours can cost many thousands of dollars in tangible losses – accompanied by latent losses of varying form.

There are other costs to consider as well. These include disruptions to internal systems that can have significant productivity impacts and costs to employees and partners. Performance penalties may be incurred due to service interruptions that impact service-level agreements (SLAs). There is the potential loss of customers' goodwill and negative publicity, which can impact brand and reputation. There may be associated liabilities and financial penalties. And, for COA, even lives could be at stake.

1. Large scale loss of employee productivity (*e.g. no access to business applications, internet, etc.*)
2. Revenue loss
3. Lost customers
4. Emergency recovery costs and associated staff overtime
5. Reduced levels of customer satisfaction
6. Negative impact to the COA/CTM brand and reputation
7. Breach of customer agreements (SLAs)
8. Exposure to legal risks

D. A preliminary current-state assessment of the CTM data center facilities concludes:

1. Significant availability risks.

2. Need for considerable capital investments to achieve longer lifecycles and higher availability structures.
3. Aging & inefficient legacy systems.
4. No ability to perform concurrent facility maintenance.
5. Lack of fault tolerance.
6. Lack of standalone data center facilities
7. Fragmented & disparate facility infrastructure

3. EXISTING DATA CENTER SPECIFICATIONS

A. COA/CTM Waller Creek Data Center

The Waller Creek Data Center is the COA/CTM's primary data center facility – housing all the centralized processing, storage, and networks that serve the COA/CTM's customer base. The Waller Creek Data Center was built in 1993 as a retrofit to the existing office structure; including segregated electrical and cooling infrastructure build-out. The data center encompasses the entire 10th floor of a 10 story office complex. Dedicated power & cooling infrastructure is spread throughout the building (e.g. rooftop, 1st level garage, etc.).

Current Operating Figures:

Racks – 46

Total UPS Protected IT Load – 100 kW

WCC Production DC Raised Floor Space – 4,000 Sq. Ft. (+ 6000 Sq. Ft. support space)

B. COA/CTM City Hall Data Center

The City Hall Data Center is COA/CTM's secondary, or backup IT facility. The site was built as part of the new construction of 2006. The City Hall Data Center has mission critical systems (like UPS, Generator, and Dedicated HVAC); however, these systems are not dedicated to exclusively support the COA/CTM data center. The site's chilled water is supplied by a city owned district chilled water plant.

Current Operating Figures:

Racks – 15

Total UPS Protected IT Load – 15 kW

Data Center Floor Space – 300 Sq. Ft.

4. TARGET STATE & RISK BENCHMARK

Based on COA/CTM's research of the subject, quantifying risk for existing data center facilities & developing improvement recommendations requires a benchmark to measure against. In other words, a standard for performance must be set before an assessment can define the gap that exists

between *what is* and *what is desired*. This “gap” represents the vulnerabilities which undermine anticipated facility reliability, and which also put the data center facility at risk of long duration downtime. For the purpose of this RFP, “COA/CTM Data Center Facilities - Target State Criteria” are outlined below to illustrate the operating criteria with which COA/CTM executive management expects its current & future data center facilities to operate within. These criteria are based on COA/CTM’s individual business needs and the industry wide data collected regarding IT organizations of COA/CTM’s size, scope, and criticality.

As can be seen below (Line A.), COA/CTM will require assistance in defining the “Tier” equivalency rating that best matches the criteria called out in lines B through F. The awarded consultant shall be asked to use industry standards, proxy organizations, and COA/CTM availability requirements to classify our desired target state as Tier I, Tier II, Tier III, or Tier IV. The motive for a “Tier” classification rating is to simplify the comparison of complex facility infrastructures for the consumption of all data center facility stakeholders and decision makers (e.g. COA planners, budget officers, executives, and council). COA/CTM has chosen the ANSI/TIA-942 standard as our benchmark for this risk assessment. COA/CTM’s use of ANSI/TIA-942 is not exclusionary, nor is it a deliverable requirement of this RFP. Other widely accepted data center standards or proprietary, vendor specific standards may be used in place of ANSI/TIA-942. However, the use of alternate standards must be accompanied by a developed explanation of why the standard was used, and how it meets or exceeds the criteria set forth in ANSI/TIA-942. Only “in-scope” domains from Section # 1 Introduction should be measured against the applied standard. Note – COA/CTM is not seeking a formal “Tier” certification of any kind.

COA/CTM Data Center Facilities - Target State Criteria

- A. Data Center Facilities Target State “Tier” – TBD
- B. Capable of supporting concurrent facilities maintenance activities (*i.e. completing regularly scheduled or emergency maintenance without affecting the critical IT load*).
- C. Capable of accommodating “lights out” operation - with no on-site staffing.
- D. Compliance with ANSI/TIA-942 – Telecommunications Infrastructure Standards for Data Centers.
- E. Capable of supporting current mission critical loads over the Next 10 years (**growth accommodations not considered at this time*)

5. STATEMENT OF WORK & ASSOCIATED DELIVERABLES

The awarded consultant must perform the following services and provide associated deliverables. Based on budgetary concerns, the Scope of Work & Associated Deliverables (section #5) should be priced independently for each in-scope data center facility (see section #3 & Pricing Worksheet).

A. Data Center Facility Target State “Tier” Development

Develop a Data Center Facilities Target State “Tier” rating (ANSI/TIA-943 or chosen equivalent) based upon analysis of:

- COA/CTM’s Target State Criteria (section #4).

- Data center facility “Tier” ratings of proxy organizations matching COA/CTM’s size, scope, and criticality (preferably public sector).
- Interviews with COA/CTM IT executives who can dictate service levels and criticality of IT services rendered from these data center facilities.
- Other applicable criteria as prescribed by awarded consultant.

Data Center Facilities Target State “Tier” report should include methodology utilized, proxy data collected, and a high level summary of why the chosen “Tier” applies to COA/CTM’s availability needs. The “Data Center Facilities Target State “Tier” Development” deliverable shall be considered complete upon COA/CTM’s written acceptance of the report. “Data Center Facilities Target State “Tier” Development” deliverable must be completed and approved in writing by COA/CTM before consultant moves to further deliverables.

From Section #4 - COA/CTM has chosen the ANSI/TIA-942 standard as our benchmark for this risk assessment. COA/CTM’s use of ANSI/TIA-942 is not exclusionary, nor is it a deliverable requirement of this RFP. Other widely accepted data center standards or proprietary, vendor specific standards may be used in place of ANSI/TIA-942. However, the use of alternate standards must be accompanied by a developed explanation of why the standard was used, and how it meets or exceeds the criteria set forth in ANSI/TIA-942. Only “in-scope” domains from Section # 1 Introduction should be measured against the applied standard. Note – COA/CTM is not seeking a formal “Tier” certification of any kind.

B. Data Center Facility Risk Assessment Report

Develop a report assessing the ongoing operational risks faced by COA/CTM in operating its current data center facilities. This report should assess the data center facility design, configuration, & capabilities in the context of industry-recognized measures of data center reliability and availability, and rank the severity of vulnerabilities found. The report should note how the characteristics of the current state data center facility does or does not meet the completed “Target State Criteria” called for in section 4 (specifically, the COA/CTM stated lifecycle criteria of 10 years).

As called for in Section #1, Line C, “Scope”, only certain realms of the data center will be covered in this report due to budgetary concerns. “In-Scope” domains are called out below with examples of risk components. These examples are not intended to be exclusionary or all encompassing – they are meant to provide a better level of understanding as to COA/CTM’s desired level of detail regarding the risk assessment report deliverable. The “Data Center Facility Risk Assessment Report” deliverable shall be considered complete upon COA/CTM’s written acceptance of the report.

1) Mission Critical Power Architecture

- Primary and Backup Power Systems Architecture, Configuration, & Placement
- Equipment Lifecycle
- Maintainability
- Failover capacity thresholds and automation structure
- Routing Diversity
- Single Points of Failure
- Termination Age
- Source Reliability

2) Mission Essential HVAC Systems

- Primary and Backup HVAC Systems Architecture, Configuration, & Placement
- Equipment Lifecycle
- Single Points of Failure
- Failover capacity thresholds and automation structure
- Maintainability
- Plumbing of chilled water, condensate, compressed air, etc.

3) Location

- Environmental Hazards
- Geographic Hazards
- Fuel Delivery
- Mission critical facilities infrastructure location & local hazard (*e.g. wet pipe above UPS plant*)
- Flood Plain
- Equipment layout and configuration
- Roof Leaks
- Integration with larger property structure & infrastructure (*neither data center is stand-alone*)

4) Data Center Environmental, Power, & Operations Monitoring Systems

- Infrastructure Visibility
- Event Response
- “Lights Out” capable operations

5) Fire Alarm and Suppression Systems

- Emergency Power Off Systems (EPO)
- Wet Pipe, Pre-Action, or Gaseous

C. Qualified Recommendations

Analyze the information collected and create high level recommendations to meet the COA/CTM's data center facility operating needs (*see section #4).

1. Recommendations Format: Develop and provide a minimum of three recommendation options for achieving COA/CTM's desired level of data center facility availability and lifecycle (*see section #4). The practicality, implementation considerations, & economic viability of all recommendations should be outlined to provide COA/CTM a high level understanding of what it will take to achieve its desired performance state.

Examples of qualified recommendations could be, but are not limited to:

- Minor Upgrades &/or facility retrofits (no downtime required to implement).
- Major Upgrades &/or facility retrofits (downtime required to implement).

- Sourcing of 3rd party provided data center facilities. (*note – new construction not considered at this time*)

At a minimum, each recommendation option should include, but not limited to, the following elements:

- 1.1 Key assumptions used for each option.
- 1.2 High level estimated costs to implement each option and key assumptions underlying those costs.
- 1.3 Benefits & drawbacks for each option – including downtime duration required to implement recommendations.

The “Qualified Recommendations” deliverable shall be considered complete upon COA/CTM’s written acceptance.

6. CONSULTANT RESPONSIBILITIES

The purpose of this section of the RFP is to describe the Consultant responsibilities.

- A. Any engineering services, electrical services, or other professional services needed to complete the scope of work and associated deliverables are to be provided by the consultant – at the consultant’s expense. No COA/CTM operating budgets shall be allocated to supplement Risk Assessment RFP needs.
- B. Upon award of the contract, the contractor shall conduct a kick-off meeting with the CTM Project Team to determine the tasks that shall be accomplished and negotiate a schedule for their completion.
- C. Any on-site consultant and/or contractor must have cleared a criminal background check before having unescorted access to city facilities or remote access via the Internet. The background check must be done by the City and must be done in person prior to the kick-off meeting.
- D. At the conclusion of the project initial planning, the Consultant shall create a project work plan including schedule (which estimates deliverable milestones and resource requirements).
- E. A draft version of each written deliverable shall be produced by Consultant for review by CTM. CTM will provide feedback and corrections so that the Consultant can publish and submit the final version.
- F. The Consultant shall conduct and document all meetings and interviews with CTM and/or City of Austin staff.
- G. Deliverables must be provided on the dates specified. Any changes to the delivery date must have prior approval (in writing) by the CTM Project Manager (City’s Contract Manager) or designate.
- H. All deliverables must be submitted in a format approved by the CTM Project Manager or designate.
- I. If the deliverable cannot be provided within the scheduled time frame, the Consultant is required to contact the CTM Project Manager or designee in writing with a reason for the delay and the proposed revised schedule. The request for a revised schedule must include the impact on related tasks and the overall project.

- J. A request for a revised schedule must be reviewed and approved in writing by the CTM Project Manager or designee before placed in effect.
- K. The Consultant is required to provide the Project Manager or designee with bi-weekly written progress reports of this project. These are due to the City's Project Manager or designate by the close of business on a mutually agreed upon day of every two weeks throughout the life of the project.
- L. The progress reports shall detail all work performed and completed during the previous two weeks for which the progress report is provided and shall present the work to be performed during the subsequent two weeks.
- M. The progress report shall identify any problems encountered or still outstanding with an explanation of the cause and resolution of the problem or how the problem will be resolved.
- N. The Consultant shall be responsible for conducting bi-weekly status meetings with the CTM Project Manager or designee. The meetings shall be held on a mutually agreed upon day, time and place of every two weeks. The meetings can be in person or over the phone at the discretion of the CTM Project Manager or designee.

7. CITY OF AUSTIN RESPONSIBILITIES

The purpose of this section of the RFP is to describe the City of Austin's responsibilities.

- A. Provide all available engineering documentation, facility documentation, floor layouts, etc. that will aid in the development of the Risk Assessment RFP SOW/Deliverables. No guarantees or obligations (on the part of COA/CTM) are implied that this documentation will be all-inclusive or accurate to the specific needs of the awarded consultant. However, every effort will be made by COA/CTM to provide available background information.
- B. Provide workspace and facilities for Consultant resources working on the project.
- C. Assign a Project Manager and core team.
- D. Resources will be available in a timely manner (as required).
- E. Staff will be available as requested for the interviews, meetings, briefings and workshops. These individuals will be experienced subject matter experts (SMEs) in the covered IT areas and will be able to make decisions as needed to advance the project.
- F. Provide meeting room facilities.
- G. Assist with scheduling COA/CTM staff and facilities.
- H. Provide access to COA/CTM systems as required in accordance with City security policies and practices.