METRO

CONTRACT NO. 200814

PLANVIEW PROJECT PORTFOLIO MANAGEMENT SOFTWARE
DIR CONTRACT NO. DIR-TSO-3763

(RFP 307649)

CONTRACTOR:	**Dell Marketing, L.P.** **One Dell Way** **Round Rock, TX 78682** **E-Mail:** heather_jones@dell.com
AWARD DATE:	**April 22, 2022**
AWARD AMOUNT:	**Not-to-Exceed: $491,415.80**
CONTRACT TERM:	**One (1) Year from Notice to Proceed** **(April 29, 2022 - April 28, 2023)**
PROJECT MANAGER:	**Jim McCune** **512-369-7560** **jim.mccune @capmetro.org**
CONTRACT ADMINISTRATOR:	**Danny Solano** **512-389-7446** **danny.solano@capmetro.org**

PROCUREMENT DEPARTMENT
CAPITAL METROPOLITAN TRANSPORTATION AUTHORITY
2910 E. 5th STREET
AUSTIN, TEXAS 78702

TABLE OF CONTENTS

CONTRACT NO. 200814

PLANVIEW PROJECT PORTFOLIO MANAGEMENT SOFTWARE
DIR CONTRACT NO. DIR-TSO-3763

(RFP 307649)

The entire contract shall consist of the cover page, the table of contents and all the documents listed on the table of contents

TAB	DESCRIPTION
1	EXHIBIT A, PRICING SCHEDULE
2	EXHIBIT B, REPRESENTATIONS AND CERTIFICATIONS
3	EXHIBIT F, SCOPE AND COMPLIANCE MATRIX
4	CONTRACTOR’S DETAILED DEPARTMENT OF INFORMATION RESOURCES QUOTES AND SOW DOCUMENTS
5	CONTRACTOR’S DEPARTMENT OF INFORMATION RESOURCES CONTRACT NUMBER DIR-TSO-3763

TAB 1

EXHIBIT A

PRICING SCHEDULE

EXHIBIT A
PRICING SCHEDULE
RFP 307649

THE OFFEROR IS REQUIRED TO SIGN AND DATE EACH PAGE OF THIS SCHEDULE

1. IDENTIFICATION OF OFFEROR AND SIGNATURE OF AUTHORIZED AGENT

Company Name (Printed)	Dell Marketing, L.P.		
Address	One Dell Way		
City, State, Zip	Round Rock, TX 78682		
Phone, Fax, Email	(512) 720-4661		Heather_Jones1@Dell.com
The undersigned agrees, if this offer is accepted within the period specified, to furnish any or all supplies and/or services specified in the Schedule at the prices offered therein.			
Authorized Agent Name and Title (Printed)	Heather Jones, Proposal Manager		
Signature and Date	Heather Jones		3/22/2022

2. ACKNOWLEDGEMENT OF AMENDMENTS

The offeror acknowledges receipt of the following amendment(s) to this solicitation (give number and date of each).

Amendment #	Date	Amendment #	Date
None at time of submission			

3. PROMPT PAYMENT DISCOUNT

# of Days	N/A	Percentage	N/A %

Note, payment terms are specified in Exhibit E, Contractual Terms and Conditions.

4. SBE OR DBE (choose one) GOAL (TO BE COMPLETED UPON AWARD BY CAPITAL METRO)

The SBE OR DBE (choose one) participation commitment for this contract is the following percentage of the total contract:

N/A %

5. AUTHORITY'S ACCEPTANCE (TO BE COMPLETED UPON AWARD BY CAPITAL METRO)

The Authority hereby accepts this offer.

Authorized Agent Name and Title (Printed)	Muhammad Abdullah, CTCM, C.P.M. Chief Contracting Officer
Signature and Date	E-SIGNED by Muhammad Abdullah on 2022-04-29 17:23:11 GMT April 29, 2022
Accepted as to:	Exhibit A, Pricing Schedule, Dated March 22, 2022, Section 7, Pricing, Base Items 1 Through 4, for a Total Not to Exceed Amount of $491,415.80

The remainder of Exhibit A – Pricing Schedule has been redacted.

For further information regarding Exhibit A, you may:

- Reach out to the Contractor directly via the Contractor contact details provided on the cover page of this contract.

OR

- Submit a public information request directly to PIR@capmetro.org.

For more information regarding the Public Information Act and submitting public information requests, follow this link to our website: https://www.capmetro.org/legal/

TAB 2

EXHIBIT B

REPRESENTATIONS CERTIFICATIONS

EXHIBIT B

REPRESENTATIONS AND CERTIFICATIONS

(LOCALLY FUNDED SUPPLY/SERVICE/CONSTRUCTION CONTRACTS)

MUST BE RETURNED WITH THE OFFER

1. TYPE OF BUSINESS

(a) The offeror operates as (mark one):

□ An individual
☒ A partnership
□ A sole proprietor
□ A corporation
□ Another entity _____

(b) If incorporated, under the laws of the State of:

Delaware.

2. PARENT COMPANY AND IDENTIFYING DATA

(a) The offeror (mark one):

☒ is
□ is not

owned or controlled by a parent company. A parent company is one that owns or controls the activities and basic business policies of the offeror. To own the offering company means that the parent company must own more than fifty percent (50%) of the voting rights in that company.

(b) A company may control an offeror as a parent even though not meeting the requirements for such ownership if the company is able to formulate, determine, or veto basic policy decisions of the offeror through the use of dominant minority voting rights, use of proxy voting, or otherwise.

(c) If not owned or controlled by a parent company, the offeror shall insert its own EIN (Employer's Identification Number) below:

(d) If the offeror is owned or controlled by a parent company, it shall enter the name, main office and EIN number of the parent company, below:

Dell Technologies Inc.
One Dell Way Round Rock, TX
78682.
[redacted]

3. CERTIFICATION OF INDEPENDENT PRICE DETERMINATION

(a) The offeror (and all joint venture members, if the offer is submitted by a joint venture) certifies that in connection with this solicitation:

(1) the prices offered have been arrived at independently, without consultation, communication, or agreement for the purpose of restricting competition, with any other offeror or with any other competitor;

(2) unless otherwise required by law, the prices offered have not been knowingly disclosed by the offeror and will not knowingly be disclosed by the offeror prior to opening of bids in the case of an invitation for bids, or prior to contract award in the case of a request for proposals, directly or indirectly to any other offeror or to any competitor; and

(3) no attempt has been made or will be made by the offeror to induce any other person or firm to submit or not to submit an offer for the purpose of restricting competition.

(b) Each signature on the offer is considered to be a certification by the signatory that the signatory:

(1) is the person in the offeror's organization responsible for determining the prices being offered in this bid or proposal, and that the signatory has not participated and will not participate in any action contrary to paragraphs (a)(1) through (a)(3) of this provision; or

(i) has been authorized, in writing, to act as agent for the following principals in certifying that those principals have not participated, and will not participate in any action contrary to paragraphs (a)(1) through (a)(3) of this provision _______ [insert full name of person(s) in the offeror's organization responsible for determining the prices offered in this bid or proposal, and the title of his or her position in the offeror's organization];

(ii) as an authorized agent, does certify that the principals named in subdivision (b)(2)(i) of this provision have not participated, and will not participate, in any action contrary to paragraphs (a)(1) through (a)(3) of this provision; and

(iii) as an agent, has not personally participated, and will not participate, in any action contrary to paragraphs (a)(1) through (a)(3) of this provision.

(c) If the offeror deletes or modifies paragraph (a)(2) of this provision, the offeror must furnish with its offer a signed statement setting forth in detail the circumstances of the disclosure.

4. DEBARMENT, SUSPENSION, INELIGIBILITY AND VOLUNTARY EXCLUSION

(a) In accordance with the provisions of 2 C.F.R. (Code of Federal Regulations), part 180, the offeror certifies to the best of the offeror's knowledge and belief, that it and its principals:

(1) are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any Federal department or agency;

(2) have not within a three (3) year period preceding this offer been convicted of or had a civil judgment rendered against them for the commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State, or local) transaction or contract under a public transaction; violation of Federal or State antitrust statutes, or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;

(3) are not presently indicted for or otherwise criminally or civilly charged by a governmental entity (Federal, State, or local) with commission of any of the offenses enumerated in (a)(2) above; and

(4) have not within a three (3) year period preceding this offer had one or more public transactions (Federal, State, or local) terminated for cause or default.

(b) Where the offeror is unable to certify to any of the statements above, the offeror shall attach a full explanation to this offer.

(c) For any subcontract at any tier expected to equal or exceed $25,000:

(1) In accordance with the provisions of 2 C.F.R. part 180, the prospective lower tier subcontractor certifies, by submission of this offer, that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any Federal department or agency.

(2) Where the prospective lower tier participant is unable to certify to the statement, above, an explanation shall be attached to the offer.

(3) This certification (specified in paragraphs (c)(1) and (c)(2), above) shall be included in all applicable subcontracts and a copy kept on file by the prime contractor. The prime contractor shall be required to furnish copies of the certifications to the Authority upon request.

5. COMMUNICATIONS

(a) All oral and written communications with the Authority regarding this solicitation shall be exclusively with, or on the subjects and with the persons approved by, the persons identified in this solicitation. Discussions with any other person not specified could result in disclosure of proprietary or other competitive sensitive information or otherwise create the appearance of impropriety or unfair competition and thereby compromise the integrity of the Authority's procurement system. If competition cannot be resolved through normal communication channels, the Authority's protest procedures shall be used for actual or prospective competitors claiming any impropriety in connection with this solicitation.

(b) By submission of this offer, the offeror certifies that it has not, and will not prior to contract award, communicate orally or in writing with any Authority employee or other representative of the Authority (including Board Members, Capital Metro contractors or consultants), except as described below:

Individual's Name	Date/Subject of Communication

(Attach continuation form, if necessary.)

6. CONTINGENT FEE

(a) Except for full-time, bona fide employees working solely for the offeror, the offeror represents as part of its offer that it (mark one):

□ has
■ has not

employed or retained any company or persons to solicit or obtain this contract, and (mark one):

□ has
■ has not

paid or agreed to pay any person or company employed or retained to solicit or obtain this contract any commission, percentage, brokerage, or other fee contingent upon or resulting from the award of this contract.

(b) The offeror agrees to provide information relating to (a) above, when any item is answered affirmatively.

7. CODE OF ETHICS

*** Dell adheres to its own internal Code of Conduct that we believe meets or exceeds the intent of the Customer's Code of Conduct. Further details on Dell's Code of Conduct can be found online at https://www.delltechnologies.com/content/dam/delltechnologies/assets/whoweare/resources/Dell%20Technologies%20Code%20of%20Conduct%20-%20English.pdf ***

(a) Statement of Purpose

The brand and reputation of Capital Metro is determined in large part by the actions or ethics of representatives of the agency. Capital Metro is committed to a strong ethical culture and to ethical behavior by all individuals serving Capital Metro as employees, members of the Board of Directors or volunteers. Individuals serving Capital Metro will conduct business with honesty and integrity. We will make decisions and take actions that are in the best interest of the people we serve and that are consistent with our mission, vision and this policy. The Code of Ethics (the “Code”) documents Capital Metro’s Standards of Ethical Conduct and policies for Ethical Business Transactions. Compliance with the Code will help protect Capital Metro’s reputation for honesty and integrity. The Code attempts to provide clear principles for Capital Metro’s expectations for behavior in conducting Capital Metro business. We have a duty to read, understand and comply with the letter and spirit of the Code and Capital Metro policies. You are encouraged to inquire if any aspect of the Code needs clarification.

(b) Applicability

The Code applies to Capital Metro employees, contractors, potential contractors, Board Members and citizen advisory committee members. Violation of the Code of Ethics may result in discipline up to and including termination or removal from the Board of Directors.

(c) Standards of Ethical Conduct

The public must have confidence in our integrity as a public agency and we will act at all times to preserve the trust of the community and protect Capital Metro’s reputation. To demonstrate our integrity and commitment to ethical conduct we will:

(1) Continuously exhibit a desire to serve the public and display a helpful, respectful manner.

(2) Exhibit and embody a culture of safety in our operations.

(3) Understand, respect and obey all applicable laws, regulations and Capital Metro policies and procedures both in letter and spirit.

(4) Exercise sound judgment to determine when to seek advice from legal counsel, the Ethics Officer or others.

(5) Treat each other with honesty, dignity and respect and will not discriminate in our actions toward others.

(6) Continuously strive for improvement in our work and be accountable for our actions.

(7) Transact Capital Metro business effectively and efficiently and act in good faith to protect the Authority’s assets from waste, abuse, theft or damage.

(8) Be good stewards of Capital Metro’s reputation and will not make any representation in public or private, orally or in writing, that states, or appears to state, an official position of Capital Metro unless authorized to do so.

(9) Report all material facts known when reporting on work projects, which if not revealed, could either conceal unlawful or improper practices or prevent informed decisions from being made.

(10) Be fair, impartial and ethical in our business dealings and will not use our authority to unfairly or illegally influence the decisions of other employees or Board members.

(11) Ensure that our personal or business activities, relationships and other interests do not conflict or appear to conflict with the interests of Capital Metro and disclose any potential conflicts.

(12) Encourage ethical behavior and report all known unethical or wrongful conduct to the Capital Metro Ethics Officer or the Board Ethics Officer.

(d) Roles and Responsibilities

It is everyone's responsibility to understand and comply with the Code of Ethics and the law. Lack of knowledge or understanding of the Code will not be considered. If you have a question about the Code of Ethics, ask.

It is the responsibility of Capital Metro management to model appropriate conduct at all times and promote an ethical culture. Seek guidance if you are uncertain what to do.

It is Capital Metro's responsibility to provide a system of reporting and access to guidance when an employee wishes to report a suspected violation and to seek counseling, and the normal chain of command cannot, for whatever reason, be utilized. If you need to report something or seek guidance outside the normal chain of command, Capital Metro provides the following resources:

(1) Anonymous Fraud Hotline – Internal Audit

(2) Anonymous Online Ethics Reporting System

(3) Contact the Capital Metro Ethics Officer, Vice-President of Internal Audit, the EEO Officer or Director of Human Resources

(4) Safety Hotline

The Capital Metro Ethics Officer is the Chief Counsel. The Ethics Officer is responsible for the interpretation and implementation of the Code and any questions about the interpretation of the Code should be directed to the Ethics Officer.

(e) Ethical Business Transactions

Section 1. Impartiality and Official Position

(1) A Substantial Interest is defined by Tex. Loc. Govt. Code, § 171.002. An official or a person related to the official in the first degree by consanguinity or affinity has a Substantial Interest in:

(i) A business entity if the person owns ten percent (10%) or more of the voting stock or shares of the business entity or owns either 10% or more or $15,000 or more of the fair market value of the business entity OR funds received by the person from the business entity exceed 10% of the person's gross income for the previous year; or

(ii) Real property if the interest is an equitable or legal ownership with a fair market value of $2,500 or more.

Capital Metro will not enter into a contract with a business in which a Board Member or employee or a Family Member of a Board Member or employee as defined in Section 8 has a Substantial Interest except in case of emergency as defined in the Acquisition Policy PRC-100 or the business is the only available source for essential goods and services or property.

(2) No Board Member or employee shall:

(i) Act as a surety for a business that has work, business or a contract with Capital Metro or act as a surety on any official bond required of an officer of Capital Metro.

(ii) Represent for compensation, advise or appear on behalf of any person or firm concerning any contract or transaction or in any proceeding involving Capital Metro's interests.

(iii) Use his or her official position or employment, or Capital Metro's facilities, equipment or supplies to obtain or attempt to obtain private gain or advantage.

(iv) Use his or her official position or employment to unfairly influence other Board members or employees to perform illegal, immoral, or discreditable acts or do anything that would violate Capital Metro policies.

(v) Use Capital Metro's resources, including employees, facilities, equipment, and supplies in political campaign activities.

(vi) Participate in a contract for a contractor or first-tier subcontractor with Capital Metro for a period of one (1) year after leaving employment on any contract with Capital Metro.

(vii) Participate for a period of two (2) years in a contract for a contractor or first-tier subcontractor with Capital Metro if the Board Member or employee participated in the recommendation, bid, proposal or solicitation of the Capital Metro contract or procurement.

Section 2. Employment and Representation

A Board Member or employee must disclose to his or her supervisor, appropriate Capital Metro staff or the Board Chair any discussions of future employment with any business which has, or the Board Member or employee should reasonably foresee is likely to have, any interest in a transaction upon which the Board Member or employee may or must act or make a recommendation subsequent to such discussion. The Board Member or employee shall take no further action on matters regarding the potential future employer.

A Board Member or employee shall not solicit or accept other employment to be performed or compensation to be received while still a Board Member or employee, if the employment or compensation could reasonably be expected to impair independence in judgment or performance of their duties.

A Board Member or employee with authority to appoint or hire employees shall not exercise such authority in favor of an individual who is related within the first degree, within the second degree by affinity or within the third degree by consanguinity as defined by the Capital Metro Nepotism Policy in accordance with Tex. Govt. Code, Ch. 573.

Section 3. Gifts

It is critical to keep an arms-length relationship with the entities and vendors Capital Metro does business with in order to prevent the appearance of impropriety, undue influence or favoritism.

No Board Member or employee shall:

(1) Solicit, accept or agree to accept any benefit or item of monetary value as consideration for the Board Member's or employee's decision, vote, opinion, recommendation or other exercise of discretion as a public servant. [Tex. Penal Code §36.02(c)]

(2) Solicit, accept or agree to accept any benefit or item of monetary value as consideration for a violation of any law or duty. [Tex. Penal Code §36.02(a)(1)]

(3) Solicit, accept or agree to accept any benefit or item of monetary value from a person the Board Member or employee knows is interested in or likely to become interested in any Capital Metro contract or transaction if the benefit or item of monetary value could reasonably be inferred as intended to influence the Board Member or employee. [Tex. Penal Code §36.08(d)]

(4) Receive or accept any gift, favor or item of monetary value from a contractor or potential contractor of Capital Metro or from any individual or entity that could reasonably be inferred as intended to influence the Board Member or employee.

Exception: Consistent with state law governing public servants, a gift does not include a benefit or item of monetary value with a value of less than $50, excluding cash or negotiable instruments, unless it can reasonably be inferred that the item was intended to influence the Board Member or employee. A department may adopt more restrictive provisions if there is a demonstrated and documented business need. [Tex. Penal Code § 36.10(a)(6)]

Exception: A gift or other benefit conferred, independent of the Board Member's or employee's relationship with Capital Metro, that is not given or received with the intent to influence the Board Member or employee in the performance of his or her official duties is not a violation of this policy. The Capital Metro Ethics Officer or Board Ethics Officer must be consulted for a determination as to whether a potential gift falls within this exception.

Exception: Food, lodging, or transportation that is provided as consideration for legitimate services rendered by the Board Member or employee related to his or her official duties is not a violation of this policy.

If you are uncertain about a gift, seek guidance from the Ethics Officer.

Section 4. Business Meals and Functions

Board Members and employees may accept invitations for free, reasonable meals in the course of conducting Capital Metro's business or while attending a seminar or conference in connection with Capital Metro business as long as there is not an active or impending solicitation in which the inviting contractor or party may participate and attendance at the event or meal does not create an appearance that the invitation was intended to influence the Board Member or employee.

When attending such events, it is important to remember that you are representing Capital Metro and if you chose to drink alcohol, you must do so responsibly. Drinking irresponsibly may lead to poor judgment and actions that may violate the Code or other Capital Metro policies and may damage the reputation of Capital Metro in the community and the industry.

Section 5. Confidential Information

It is everyone's responsibility to safeguard Capital Metro's nonpublic and confidential information.

No Board Member or employee shall:

(1) Disclose, use or allow others to use nonpublic or confidential information that Capital Metro has not made public unless it is necessary and part of their job duties and then only pursuant to a nondisclosure agreement approved by legal counsel or with consultation and permission of legal counsel.

(2) Communicate details of any active Capital Metro procurement or solicitation or other contract opportunity to any contractor, potential contractor or individual not authorized to receive information regarding the active procurement or contract opportunity.

Section 6. Financial Accountability and Record Keeping

Capital Metro's financial records and reports should be accurate, timely, and in accordance with applicable laws and accounting rules and principles. Our records must reflect all components of a transaction in an honest and forthright manner. These records reflect the results of Capital Metro's operations and our stewardship of public funds.

A Board Member or employee shall:

(1) Not falsify a document or distort the true nature of a transaction.

(2) Properly disclose risks and potential liabilities to appropriate Capital Metro staff.

(3) Cooperate with audits of financial records.

(4) Ensure that all transactions are supported by accurate documentation.

(5) Ensure that all reports made to government authorities are full, fair, accurate and timely.

(6) Ensure all accruals and estimates are based on documentation and good faith judgment.

Section 7. Conflict of Interest

Employees and Board Members are expected to deal at arms-length in any transaction on behalf of Capital Metro and avoid and disclose actual conflicts of interest under the law and the Code and any circumstance which could impart the appearance of a conflict of interest. A conflict of interest exists when a Board Member or employee is in a position in which any official act or action taken by them is, may be, or appears to be influenced by considerations of personal gain rather than the general public trust.

Conflict of Interest [Tex. Loc. Govt. Code, Ch. 171 & 176, § 2252.908]

No Board Member or employee shall participate in a matter involving a business, contract or real property transaction in which the Board Member or employee has a Substantial Interest if it is reasonably foreseeable that an action on the matter would confer a special economic benefit on the business, contract or real property that is distinguishable from its effect on the public. [Tex. Loc. Govt. Code, § 171.004]

Disclosure

A Board Member or employee must disclose a Substantial Interest in a business, contract, or real property that would confer a benefit by their vote or decision. The Board Member or employee may not participate in the consideration of the matter subject to the vote or decision. Prior to the vote or decision, a Board Member shall file an affidavit citing the nature and extent of his or her interest with the Board Vice Chair or Ethics Officer. [Tex. Loc. Govt. Code, § 171.004]

A Board Member or employee may choose not to participate in a vote or decision based on an appearance of a conflict of interest and may file an affidavit documenting their recusal.

Section 8. Disclosure of Certain Relationships [Tex. Loc. Govt. Code, Ch. 176]

Definitions

(1) A Local Government Officer is defined by Tex. Loc. Govt. Code § 176.001(4). A Local Government Officer is:

(i) A member of the Board of Directors;

(ii) The President/CEO; or

(iii) A third party agent of Capital Metro, including an employee, who exercises discretion in the planning, recommending, selecting or contracting of a vendor.

(2) A Family Member is a person related within the first degree by consanguinity or the second degree by affinity as defined by Tex. Govt. Code, Ch. 573.

(3) A Family Relationship is a relationship between a person and another person within the third degree by consanguinity or the second degree by affinity as defined by Tex. Govt. Code, Ch. 573.

(4) A Local Government Officer must file a Conflicts Disclosure Statement (FORM CIS) if:

(i) The person or certain Family Members received at least $2,500 in taxable income (other than investment income) from a vendor or potential vendor in the last twelve (12) months through an employment or other business relationship;

(ii) The person or certain Family Members received gifts from a vendor or potential vendor with an aggregate value greater than $100 in the last 12 months; or

(iii) The vendor (or an employee of the vendor) has a Family Relationship with the Local Government Officer.

(5) A vendor doing business with Capital Metro or seeking to do business with Capital Metro is required to file a completed questionnaire (FORM CIQ) disclosing the vendor's affiliations or business relationship with any Board Member or local government officer or his or her Family Member.

Section 9. Duty to Report and Prohibition on Retaliation

Board Members and employees have a duty to promptly report any violation or possible violation of this Code of Ethics, as well as any actual or potential violation of laws, regulations, or policies and procedures to the hotline, the Capital Metro Ethics Officer or the Board Ethics Officer.

Any employee who reports a violation will be treated with dignity and respect and will not be subjected to any form of retaliation for reporting truthfully and in good faith. Any retaliation is a violation of the Code of Ethics and may also be a violation of the law, and as such, could subject both the individual offender and Capital Metro to legal liability.

Section 10. Penalties for Violation of the Code of Ethics

In addition to turning over evidence of misconduct to the proper law enforcement agency when appropriate, the following penalties may be enforced:

(1) If a Board Member does not comply with the requirements of this policy, the Board member may be subject to censure or removal from the Board in accordance with Section 451.511 of the Texas Transportation Code.

(2) If an employee does not comply with the requirements of this policy, the employee shall be subject to appropriate disciplinary action up to and including termination.

(3) Any individual or business entity contracting or attempting to contract with Capital Metro which offers, confers or agrees to confer any benefit as consideration for a Board Member's or employee's decision, opinion, recommendation, vote or other exercise of discretion as a public servant in exchange for the Board Member's or employee's having exercised his official powers or performed his official duties, or which attempts to communicate with a Board Member or Capital Metro employee regarding details of a procurement or other contract opportunity in violation of Section 5, or which participates in the violation of any provision of this Policy may have its existing Capital Metro contracts terminated and may be excluded from future business with Capital Metro for a period of time as determined appropriate by the President/CEO.

(4) Any individual who makes a false statement in a complaint or during an investigation of a complaint with regard to a matter that is a subject of this policy is in violation of this Code of Ethics and is subject to its penalties. In addition, Capital Metro may pursue any and all available legal and equitable remedies against the person making the false statement or complaint.

Section 11. Miscellaneous Provisions

(1) This Policy shall be construed liberally to effectuate its purposes and policies and to supplement such existing laws as they may relate to the conduct of Board Members and employees.

(2) Within sixty (60) days of the effective date for the adoption of this Code each Board Member and employee of Capital Metro will receive a copy of the Code and sign a statement acknowledging that they have read, understand and will comply with Capital Metro's Code of Ethics. New Board Members and employees will receive a copy of the Code and are required to sign this statement when they begin office or at the time of initial employment.

(3) Board Members and employees shall participate in regular training related to ethical conduct, this Code of Ethics and related laws and policies.

8. RESERVED

9. TEXAS ETHICS COMMISSION CERTIFICATION

In accordance with Section 2252.908, Texas Government Code, upon request of the Authority, the selected contractor may be required to electronically submit a "Certificate of Interested Parties" with the Texas Ethics Commission in the form required by the Texas Ethics Commission, and furnish the Authority with the original signed and notarized document prior to the time the Authority signs the contract. The form can be found at www.ethics.state.tx.us. Questions regarding the form should be directed to the Texas Ethics Commission.

10. TEXAS LABOR CODE CERTIFICATION (CONSTRUCTION ONLY)

Contractor certifies that Contractor will provide workers' compensation insurance coverage on every employee of the Contractor employed on the Project. Contractor shall require that each Subcontractor employed on the Project provide workers' compensation insurance coverage on every employee of the Subcontractor employed on the Project and certify coverage to Contractor as required by Section 406.96 of the Texas Labor Code, and submit the Subcontractor's certificate to the Authority prior to the time the Subcontractor performs any work on the Project.

11. CERTIFICATION REGARDING ISRAEL

As applicable and in accordance with Section 2270.002 of the Texas Government Code, the Contractor certifies that it does not boycott Israel and will not boycott Israel during the term of this Contract.

12. CERTIFICATION REGARDING FOREIGN TERRORIST ORGANIZATIONS

Contractor certifies and warrants that it is not engaged in business with Iran, Sudan, or a foreign terrorist organization, as prohibited by Section 2252.152 of the Texas Government Code.

13. VERIFICATION REGARDING FIREARM ENTITIES AND FIREARM TRADE ASSOCIATIONS

As applicable and in accordance with Section 2274.002 of the Texas Government Code, Contractor verifies that it does not have a practice, policy, guidance, or directive that discriminates against a firearm entity or firearm trade association and will not discriminate during the term of the Contract against a firearm entity or firearm trade association.

14. BOYCOTT OF ENERGY COMPANIES PROHIBITED

Pursuant to Chapter 2274 of Texas Government Code, Contractor verifies that:

(a) it does not, and will not for the duration of the Contract, boycott energy companies, as defined in Section 2274.002 of the Texas Government Code, or

(b) the verification required by Section 2274.002 of the Texas Government Code does not apply to Contractor and this Contract. If circumstances relevant to this provision change during the course of the Contract, Contractor shall promptly notify the Authority.

15. CRITICAL INFRASTRUCTURE PROHIBITION

Pursuant to Chapter 2274 of Texas Government Code, Contractor certifies that, if this Contract or any contract between Contractor and Capital Metro relates to critical infrastructure, as defined in Chapter 2274 of the Texas Government Code, Contractor is not owned by or the majority of stock or other ownership interest of its firm is not held or controlled by:

(a) individuals who are citizens of China, Iran, North Korea, Russia, or a Governor-designated country; or

(b) a company or other entity, including a governmental entity, that is owned or controlled by citizens of or is directly controlled by the government of China, Iran, North Korea, Russia, or a Governor-designated country; or

(c) headquartered in China, Iran, North Korea, Russia, or a Governor-designated country.

16. CERTIFICATION OF PRIME CONTRACTOR PARTICIPATION

(a) The Prime Contractor certifies that it shall perform no less than thirty percent (30%) of the work with his own organization. The on-site production of materials produced by other than the Prime Contractor's forces shall be considered as being subcontracted.

(b) The organization of the specifications into divisions, sections, articles, and the arrangement and titles of the project drawings shall not control the Prime Contractor in dividing the work among subcontractors or in establishing the extent of the work to be performed by any trade.

(c) The offeror further certifies that no more than seventy percent (70%) of the work will be done by subcontractors.

17. REPRESENTATION REGARDING CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT

(a) *Prohibition.* This Contract is subject to the Public Law 115-232, Section 889, and 2 Code of Federal Regulations (CFR) Part 200, including §200.216 and §200.471 related to the prohibition of certain "covered telecommunications equipment and services", which includes:

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities)

(2) For the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities).

(3) Telecommunications or video surveillance services provided by such entities or using such equipment.

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

(b) *Procedures.* The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (https://www.sam.gov) for entities excluded from receiving federal awards for "covered telecommunications equipment or services".

(c) *Representation.* The Offeror represents that—

(1) It

□ will
■ will not

provide covered telecommunications equipment or services to the Authority in the performance of any contract, subcontract or other contractual instrument resulting from this solicitation. The Offeror shall provide the additional disclosure information required at paragraph (e)(1) of this section if the Offeror responds "will" in paragraph (d)(1) of this section; and

(2) After conducting a reasonable inquiry, for purposes of this representation, the Offeror represents that—

□ does
■ does not

use covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services. The Offeror shall provide the additional disclosure information required at paragraph (e)(2) of this section if the Offeror responds "does" in paragraph (d)(2) of this section.

(d) *Disclosures.*

(1) Disclosure for the representation in paragraph (d)(1) of this provision. If the Offeror has responded "will" in the representation in paragraph (d)(1) of this provision, the Offeror shall provide the following information as part of the offer:

(i) For covered equipment—

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the original equipment manufacturer (OEM) or a distributor, if known);

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(ii) For covered services—

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the Product Service Code (PSC) of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(2) Disclosure for the representation in paragraph (d)(2) of this provision. If the Offeror has responded "does" in the representation in paragraph (d)(2) of this provision, the Offeror shall provide the following information as part of the offer:

(i) For covered equipment—

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the OEM or a distributor, if known);

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

(ii) For covered services—

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the PSC of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

18. SIGNATURE BLOCK FOR ALL REPRESENTATIONS AND CERTIFICATIONS

(a) These representations and certifications concern a material representation of fact upon which reliance will be placed in awarding a contract. If it is later determined that the offeror knowingly rendered an erroneous or false certification, in addition to all other remedies the Authority may have, the Authority may terminate the contract for default and/or recommend that the offeror be debarred or suspended from doing business with the Authority in the future.

(b) The offeror shall ~~provide immediate written notice to the Authority~~ if, at any time prior to contract award, the offeror learns that the offeror's certification was, or a subsequent communication makes, the certification erroneous.

*Dell will notify SAM of any changes in status. Dell cannot notify all customers individually.

(c) Offerors must set forth full, accurate and complete information as required by this solicitation (including this attachment). Failure of an offeror to do so may render the offer nonresponsive.

(d) A false statement in any offer submitted to the Authority may be a criminal offense in violation of Section 37.10 of the Texas Penal Code.

(e) I understand that a false statement on this certification may be grounds for rejection of this submittal or termination of the awarded contract.

Name of Offeror:

Dell Marketing L.P.

Type/Print Name of Signatory:

Heather Jones, Proposal Manager

Signature:

Heather Jones

Date:

2/28/22

TAB 3

EXHIBIT F

SCOPE AND COMPLIANCE MATRIX

Exhibit F - Project Portfolio Management System Scope and Compliance Tracebility Matrix

A	The Contractor is required to indicate the compliance status relative to each individual requirement listed in the Compliance Matrix by marking C-can comply; N-cannot comply, A-will comply with an alternative Responses of "C" or "N" do not require any further elaboration A response of "A" requires an explanation					
B	The Comments section shall be used for "A-will comply with an alternative" for explaining the alternative Do not add comments for "C" or "N" Questions on the Compliance Matrix should be directed to the Contracts Administrator prior to submitting					
C	The Contractor must deliver a system encompassing all requirements including delivery of third-party products to make the solution fully functional					
D	Sections 1 through 4 contain clauses from Exhibit F sections 1 through 3, and are presented for the Contractor to respond with compliance					
E	The Final Column entitled "Test #" will be used during the Develop Phase when the Contractor will update the Compliance Matrix with the test number that responds with each line					
#	**Compliance Matrix**	**Compliance**	**Proposer Questions**	**Capital Metro Response**	**Proposer Comments**	**Test #**
1.0 Changed in Amendment 1	**Introduction**. Capital Metropolitan Transportation Authority ("Capital Metro") is requesting proposals for services to provide, and integrate a commercial off-the-shelf (COTS) Enterprise Project Portfolio Management system (hereinafter "PPM System") to replace its current Enterprise Project Portfolio Management (hereinafter "EPPM") Tool. This project will procure and implement a PPM system to replace the current EPPM tool and provide a two-way, real-time integration with the Oracle ERP system that is being implemented while we continue to use MS Project or approved equivalent as our enterprise-wide scheduling tool. The system will provide predictive analytics to help ensure enterprise-wide strategy-to-execution alignment and adaptation.					
1.1 Changed in Amendment 1	**Implementation Approach.** The implementation approach will incorporate the agency's Enterprise Project Portfolio Management framework, program and maturity path. The selected Contractor (hereinafter the "Contractor") shall supply any required software and all proper and necessary licenses and services to fully configure, and integrate the PPM System into the existing environment. The approach must maximize the out of the box functionality of a PPM system to minimize development of customizations and complexity for future supportability and upgradability. CapMetro expects the proposal to include an implementation schedule, and that the contractor will provide the resources needed for a successful transition to the software solution.					
1.2	**Background.** Capital Metro connects people, jobs and communities by providing Central Texans with safe, high-quality and sustainable transportation alternatives. The agency provides 30 million rides annually on its buses, trains, paratransit and vanpool vehicles and serves a population of more than 1.2 million in its 543-square-mile service area. The region's transportation leader, Capital Metro has invested in transit services like its High-Frequency Network, which move more people, more reliably, as well as its innovative on-demand service Pickup. Capital Metro is committed to increasing regional mobility and, through Project Connect, will transform how people travel throughout Central Texas. Visit capmetro.org for more information.					
1.3	**Current Project Portfolio Management Environment:** The current EPPM tool uses Microsoft Project Portfolio Management Software - Project Online integrated with four other Microsoft products: Project Web App (PWA), Power BI, SharePoint, and Dynamics AX to provide a centralized repository for conducting capital project portfolio management activities and project management delivery. Capital Metro implemented an EPPM framework with processes based on the Project Management Institute (PMI) Project Management Body of Knowledge ("PMBOK"). The EPPM framework defines the business processes and governance based on types and thresholds. The financial system of record for Capital Metro and for project accounting is currently Microsoft Dynamics AX ("AX") supported by Tyler Technologies, which is currently being replaced with Oracle using integration services of Application Software Technology, ("AST") . If there is any configuration change, customization or code development within Oracle, contractor needs to identify & provide full technical, functional, UI/prototype, security, segregation of duties, reports and other details along with comprehensive test scripts for specific tasks and deliverables that will implement. Contractor needs to work closely with the AST team to ensure that the integration works as required and to obtain all documentation that would be included with Contractors own system documentation. Project managers also use Office 365 Microsoft SharePoint ("SharePoint") to store project documents as its record keeping system of record.					
1.4	**Key System Benefits.** The key benefits envisioned for the EPPM tool and to be realized with the replacement of the EPPM tool with the PPM System include: •Increasing project visibility across the organization, resulting in better cross-department planning and execution, •Providing enterprise portfolio data and reports to facilitate prioritization, rebalancing and management of the portfolio, •Automating project management processes to improve team collaboration and project execution, •Streamlining and standardizing project proposals to support annual board funding and planning processes, and •Improving project planning, execution and closing process with defined Workflow, Change Request process etc. to optimize our investments The EPPM tool (now) and the PPM system (to be) provide a required component of the EPPM program of people, processes, technology, financial management, and relationships (project and resource dependencies).					

#	Compliance Matrix	Compliance	Proposer Questions	Capital Metro Response	Proposer Comments	Test #
1.5 Changed in Amendment 1	**EPPM Program Governance:** The Capital Metro EPPM program governance includes an Advisory Committee (AC) and a Steering Committee (SC). The Capital Metro Project Manager for this project will ensure the engagement of these committees as needed in the success of this project and alignment of the PPM system with the EPPM program.					
2.0	**PPM System Functional Requirements**					
2.1	**Functional requirements.** The requirements in this Exhibit F Scope of Services and Compliance Matrix are functional in nature and do not encompass all requirements. The selected Contractor shall supply all services to fully configure, integrate, and implement the PPM system. The Contractor shall determine, through the Plan and Design phases, the impacts to the rest of the system and specific technical modifications needed to carry out the intent herein. The Contractor shall document and discuss said needs with Capital Metro and implement the final agreed-upon solution accordingly.					
2.2 Changed in Amendment 1	**SaaS Solution.** Capital Metro prefers a Software-as-a-Service software solution. The solution will be subject to the requirements as defined herein and other sections of the contract. ~~The PPM System will be subject to Exhibit IT (Hosted Solutions) - Additional Terms and Conditions for the Performance of Information Technology (IT) Products and Services.~~					
2.3	**Integrations.** This project aims to integrate the new PPM System with other Capital Metro software. APIs are included as deliverables. See section 8.12 for additional information.					
2.4	**Systems Environment.** Capital Metro uses several systems that provide project management data e.g. estimated budgets, actual, task tracking, change management and project/portfolio health statuses. Capital Metro has limited documentation on APIs for 3rd party products. Contractor is responsible for coordinating with these vendors to obtain any information and assistance needed. All costs associated with integration between the EPPM software and Capital Metro systems shall be borne by the Contractor. Capital Metro's systems that contain fare information to include but not limited to:					
2.4.1	Client computers: Microsoft Windows 10 64bit (and above) with Microsoft Office 2016 (and above), Microsoft 365 applications including Word, Excel, PowerPoint, Outlook, MS Project					
2.4.2	Browser: MS Edge, Google Chrome					
2.4.3	Servers: Microsoft Server 2016, 64bit (and above); Server 2019 preferred					
2.4.4	Databases: Microsoft SQL Server 2016, 64bit (and above); SQL Server 2019 preferred					
2.4.5	VMware ESXi, 6.7 (and above) for server virtualization					
2.4.6	Antivirus: McAfee Endpoint Security Platform and McAfee Security Threat Protection Version 10.7 (and above)					
2.4.7	Citrix XenApp LTSR 1912 (and above)					
2.4.8	Oracle Fusion Cloud Enterprise Resource Planning (ERP)					
2.4.9	MS Dynamics AX (2012 R3) is currently being replaced by Oracle Financials. The Project Development Approach will be to schedule the Oracle and PPM System integrations so that no double entry, parallel system maintenance, and/or financial system data workarounds' will be required. It is listed here as a possible, low probability temporary integration contingency for the Contractor to acknowledge that may be discussed as a change request in the future.					
2.4.10	Power BI Professional and Microsoft Azure Services; additionally CapMetro also has a ITS2009 Data Warehouse and Business Intelligence project being implemented that may require future integration development approach that may be discussed as a change request in the future.					
2.6	**Data Migration**.					
2.6.1 Changed in Amendment 1	All EPPM tool data will be migrated by the Contractor into the PPM system, but not the data from completed projects. Data migrated to include: MS Project, Project scope, Strategic business alignment, Basic project information (Project number/name, Department, PM, Business Owner, Project Champion, Senior Executive), and Operating / Replacement Costs. Sharepoint Enterprise Site documents such as Project Charter, Contracts, and many others will stay in Sharepoint for both active and closed projects. The Contractor must provide the labor for migration activities with limited support from CapMetro due to resource constraints in this area					
2.7	**Data Archiving/Disaster Recovery/System Availability**. The solution shall meet or exceed Capital Metro's required availability and recovery requirements:					
2.7.1	System meet uptime requirement of 99.9%					

#	Compliance Matrix	Compliance	Proposer Questions	Capital Metro Response	Proposer Comments	Test #
2.7.2	Downtime procedures for scheduled maintenance windows or outages with option for after regular office hours as needed.					
2.7.3	Disaster recovery plan and data archiving processes					
2.7.4	Security Plan to include but not limited to: Data breach process, Auditing schedule, Standards used, Data Privacy process					
2.7.5	System must provide a process to archive data into Microsoft SharePoint which is our legal archiving system of record.					
3.0-7.0	**EPPM Phase Tasks and Deliverables - Reference Appendix A**					
8.0	**Functional Requirements.**					
8.1	**General System Functionality**					
~~8.1.2~~ Deleted in Amendment 1	~~Software as a Service Option available~~					
8.1.3	Intuitive modern interface					
8.1.4	System is fully documented and in-context web based help is available for all functions					
8.1.5	Powerful search capability and ability to search for user defined fields					
8.1.6	Centralized administration function allowing administrative users to easily perform advanced system configuration					
8.1.7	Provide for the migration of all project data that resides in current systems including financial information / transactions and to link Authority SharePoint associated documentation to the system					
8.1.8	Provide tools to support consistent PMBOK-based EPPM management of projects					
8.1.9	System workflows must show date and time of decisions made and allow for notes to be included with workflow; All workflow stages and notes should be viewable including the current stage and approval status					
8.2	**Project Proposal/Initiation/Plan**					
8.2.1	Create standardized, automated project proposals with corresponding data, content and business rules that can be approved converted into active projects through auditable workflow processes throughout the project management / lifecycle					
8.2.2	Create and manage project proposals across fiscal years supporting a variety of project types such as capital, operating and work-orders (non-capital expenditures)					
8.2.3	Create project proposals that can be assign multiple projects to a grant and multiple grants to a project					
8.2.4	Rank and provide portfolio project prioritization for projects, programs and proposals on one or more sets of user-defined criteria for selection criteria					
8.2.5	Rank and provide portfolio project prioritization for projects, programs and proposals on one or more sets of criteria for program or portfolio optimization on demand throughout the year					
8.2.6	Provide analysis and prioritization activities that includes user-defined drivers, prioritization of drivers, and analyzation by drivers					
8.2.7	Analyze selected or the entire portfolio of projects by budget constraints (e.g. by current fiscal year, five-year CIP, funding resource					
8.2.8	Define dependencies among projects and programs, for example, project X may only be selected if project Y is selected					
8.2.9	Adjust project processes based on the size and/or type of the project (e.g., total project amount, project length					
8.2.10	Support the development of a project management plan that includes: a scope management plan, a project team / resource management plan, a schedule management plan that includes creation of a work breakdown structure (WBS), a budget / financial management plan that references the detailed schedule and milestone payment plan, a communications management plan, a risk management plan, a procurement plan, a document control plan, a quality management plan that includes establishment of system components and integration test plan, system metrics and metric checklists, and an operations maintenance plan					
8.2.11	Include workflow for the development of project artifacts including but not limited to: Strategic Impact/Alignment, Project Charter, Roles and Responsibilities, Backlog, Change Log, Issue Log (aka Action Items and Issues Log / AIL), Risk Factors, Risk Register, Stakeholder Register, and Project Management Plan (see above)					
8.2.12	Create and maintain an organizational hierarchy within the PPM System or through integration to external directories					
8.2.13	Stage gate approval process for project requests / proposals					
8.2.14	Ability to estimate resource labor costs and revenue potential at the project request/proposal stage					
8.2.15	Ability to expose or hide configurable fields in the project request form					
8.2.16	Ability to enable and automate project request and change request workdflow approval order and notifications					
8.2.17	Support "proposed" projects not yet approved: for reporting on what-if scenarios and projections					

#	Compliance Matrix	Compliance	Proposer Questions	Capital Metro Response	Proposer Comments	Test #
8.2.18	Support multiple configurable request types (e.g., new project request, change request, etc.)					
8.2.19	Attach documents to requests					
8.3	**Project Portfolio Management**					
8.3.1	Create user definable portfolios					
8.3.2	Categorize Portfolios as a separate entity type					
8.3.3	Many-to-Many relationships between Projects and Portfolios					
8.3.4	Many-to-Many relationships between Portfolios and other entities such as vendors, assets, and projects to facilitate portfolio analysis and strategy					
8.3.5	Track and manage project dependencies to other projects, programs and portfolios					
8.3.6	Provide portfolio balancing, project and program benefit maps, prioritization/ranking and optimizing the portfolio as needed throughout the year, what-if analysis with associated reports and dashboards. The system has the ability to accommodate project prioritization and balancing against available funds and resources. System must accomodate business processes for capturing all the project previous years expenditures, current year budget and expenditures, 5-year Capital Improvement Fund budget years 1 to 5 summary years and total of year 1 to 5, and the Long Range Financial Plan which includes years 6 through 20 as part of the budgeting process.					
8.3.7	Monitor project quality, document inspections and testing results, resolve test failures and manage punch lists					
8.3.8	Maintain and update an actions / issues log, risk registry, and documentation for project team meetings and steering committee meetings and					
8.3.9	Group related projects by any project type, program, portfolio attribute					
8.3.10	Associate projects to the organizational structure (business unit, division, etc.)					
8.3.11	Roll up budgets and costs from projects to portfolios and departments, etc.					
8.3.12	Map projects to corporate objectives					
8.3.13	Automate a project closeout checklist and store closeout data within the system; ability to provide access to users to view and edit the closeout checklists during the closeout process					
8.3.14	Track the project closeout process and document the activities and approvals with a dynamic workflow system					
8.3.15	Generate Project Manager notifications when project is undergoing closeout and provide users a historical overview of the project in closeout					
8.3.16	Support historical database for searches and reports to allow for continuous improvement of project and portfolio for future projects					
8.3.17	Allow for project classification, filtering, and sorting by type and other characteristics - please describe these capabilities					
8.4	**Application Portfolio Management**					
8.4.1	Supports Application Portfolio Management					
8.4.2	Ability to capture custom attributes for applications such as Architecture Attributes, Maintenance Renewal Date, etc.					
8.4.3	Ability to create many-to-many relationships between applications and other entities such as projects, assets, business capabilities, etc.					
8.4.4	Application level dashboards to facilitate application level reporting					
8.4.5	Ability to roll-up costs and resource utilization from projects					
8.4.6	Ability to track time directly to applications					
8.4.7	Ability to upload and categorize attachments to applications (contracts, architecture diagrams, etc.)					
8.4.8	Supports Gartner's TIME methodology					
8.4.9	Ability to capture application costs such as maintenance costs, etc.					
8.4.10	Ability to calculate total cost of ownership for each application (including vendor costs and internal maintenance and support cost					
8.5	**Resource Management**					
8.5.1	Allow resource managers the ability to add, remove resources available in the resource pools and manage hours available to work on projects					
8.5.2	Track resource rates					
8.5.3	Allocate resources to a project (top-down) by hours or FTE					
8.5.4	Schedule resources to tasks, then roll estimates up to the project					
8.5.5	View resource allocations and schedules across projects					

#	Compliance Matrix	Compliance	Proposer Questions	Capital Metro Response	Proposer Comments	Test #
8.5.6	Instantaneous what-if analysis on resource supply and demand					
8.5.7	Automated resource utilization calculations for individuals and roles					
8.5.8	Automated labor costing and roll-ups by project, business unit, portfolio, etc.					
8.5.9	Capture contact and other HR information in resource profile					
8.5.10	Resource skill inventory and tracking					
8.5.11	Resource capacity vs. demand reporting					
8.5.12	Corporate level calendaring to track corporate holidays and standard time off					
8.5.13	Individual resource level calendaring to reflect events such as vacation, PTO, sick leave, etc. and reduce individual resource availability					
8.5.14	Utilization tracking (planned vs. actual), (planned vs. scheduled) & (scheduled vs. actual)					
8.6	**Predictive Planning and Forecasting**					
8.6.1	Automated resource scheduling based on configurable optimization criteria (such as score, NPV, ROI, etc.)					
8.6.2	Analyze project scheduling to include cost load / Estimates At Completion, actual costs, remaining costs, encumbrances, fiscal month, fiscal quarter, fiscal year, % complete, start, finish, actual start, actual finish, predecessors, successors resource loading, resource leveling, critical path, Gantt					
8.6.3	Leverage user-configured project checklists, capture and track previous task orders, capture unspent budget from the previous fiscal year and allow for an automatic roll over to the next fiscal year that can be turned on or off (automatic rollover is currently disallowed as a business process, but we need capability for future allowance)					
8.6.4	Scenario builder that takes into account resource and budget constraints					
8.6.5	Ability to make iterative adjustments to scenarios and to understand the impact of those adjustments to support changing business priorities					
8.6.6	Ability to compare scenarios					
8.6.7	Scenarios visually display included and excluded projects in an easy to consume format					
8.6.8	Scenarios include exclusion reasons for excluded projects					
8.6.9	Scenarios include heatmap view of resource capacity by role or named resource					
8.6.10	Scenarios include schedule view displaying originally scheduled dates and recommended scheduled dates for projects					
8.7	**Time and Expense**					
8.7.1	Pull time and expense data from the Oracle Fusion Cloud to provide actual time recorded on time sheets that has been charged to the project.					
8.8	**Project Management**					
8.8.1	Planned vs. actual summaries for hours and costs					
8.8.2	Milestone Summaries - Payment, Deliverable, Task, Key					
8.8.3	Configurable reportable user defined fields on projects or tasks					
8.8.4	Dynamic Project Gantt charts					
8.8.5	Four types of task dependencies (F2S, S2S, F2F, S2F)					
8.8.6	Ability to take baseline snapshots of project information and compare baselines vs. other baselines and baselines vs. current state					
8.8.7	Summary tasks automatically roll up subtask data					
8.8.8	Ability to add notes to workflow actions for reviewers before approval and response if item is returned					
8.8.9	Interface with MS Project or approved equivalent					
8.8.10	Facilitate the use of external Contractors by allowing external users to provide data including task and status updates to schedule, risks, action items and issues list					
8.8.11	Ability to copy/move/paste tasks within projects and/or between projects					
8.8.12	Provide hierarchical task plan/WBS with target and actual delivery dates					
8.8.13	Permit any project plan to become a template					
8.8.14	Ability to define project templates that include standard sets of tasks, standard role based resource estimates, standard documentation, and standard calendars					
8.8.15	Create new projects from templates					
8.8.16	Assign multiple resources to a task with estimated hours for each role and resource					

#	Compliance Matrix	Compliance	Proposer Questions	Capital Metro Response	Proposer Comments	Test #
8.8.17	Provide security permissions for tasks					
8.8.18	Provide collaboration tools to include but not be limited to notify resources via email when assigned to a task; provide ability for team members including external contractors to updates to task dates, percent complete, resources, notes; provide a desciption of system collaboration tools					
8.8.19	Allow permissions to distinguish project members by role to manage (create, edit, delete, view, update) projects, tasks, issues, documents					
8.8.20	Provide budget request in PPM System with ability to integrate into Oracle budget request; the APPROVED budget will be created, approved and flow from Oracle and must flow into the PPM system project. The PPM system wil track the budget vs. actuals from the inception date, create a project forecast along fiscal year or other than fiscal year basis; reflect Oracle data for assignment of grants to multiple projects and multiple grants to a project; support capital contribution from a private or public partner and contribution to a project (e.g. asset gifted to a local government)					
8.8.21	Ability to add attachments to a task					
8.9	**Issue/Risk Management**					
8.9.1	Associate issues, risks or action items to projects or tasks					
8.9.2	View, report, and track issues across projects/programs					
8.9.3	Assign issues to individuals to include external vendor team members					
8.9.4	Notify assignee and/or PM by email when issues are created, assigned or completed					
8.9.5	Include link to the issue in an automated email					
8.9.6	Permit some issues to be private for team members only					
8.9.7	Drill up from the issue to the project or task					
8.9.8	Drill down from the project or task to the issue					
8.9.9	Categorize issues (i.e.: issue "types")					
8.9.10	Permit user-defined probability and impact levels					
8.9.11	Report a single project's issues and risks					
8.9.12	Support issue and risk reporting across a portfolio or group of projects					
8.9.13	Allows configurable user defined fields in both issues and risks					
8.9.14	Capture project action items with due dates and ownership					
8.9.15	Support project risk assessment and risk mitigation planning, including the quantification of project risk					
8.10	**Financial & Budget Management**					
8.10.1	Provide ability to capture estimates of hours, costs and revenue					
8.10.2	Report actuals for hours, costs and revenue					
8.10.3	Report project finances by task, phase, milestone, project, program, account, etc.					
8.10.4	Provide project-to-date reporting					
8.10.5	Distinguish between capital and non-capital costs on a project; system must distinguish between gran t and non-grant funding included on a project and for multiple types of grants (e.g. state grant vs. federal grant)					
8.10.6	Permit capital and operating expenses on the same project					
8.10.7	Rollup sums, min, max, averages, differences in real time within views and/or reports					
8.10.8	Track budget planned and actual spend over a period of time					
8.11	**Reporting/Dashboards**					
8.11.1	Provide user-specific, configurable, real-time dashboards: Users should be able to apply filter parameters and save them into their profiles to be reused by default. All calculations and formulas should be documented and viewable by users in order to better check any report issues.					
8.11.2	Allow users the abilty to create reports and save report parameters to users profile so that it can be reused.					
8.11.3	Provide system calculations for reports and dashboards so that users can troubleshoot reporting issues.					
8.11.4	Provide intuitive report builder with drag and drop report writing functionality					
8.11.5	Capability to report on user defined fields					
8.11.6	Support calculated fields with advanced logic such as nested "if statements"					
8.11.7	Ability to perform calculations in reports such as min, max, sum, and average					

#	Compliance Matrix	Compliance	Proposer Questions	Capital Metro Response	Proposer Comments	Test #
8.11.8	Summarize financial information for organization, department, account, program, etc.					
8.11.9	Drill down from reports and dashboards to sub or related/supporting dashboards, reports					
8.11.10	Track and report status of portfolios, projects, or tasks					
8.11.11	Track and report project health with project status reports					
8.11.12	Reporting outputs include List reports, cross tab reports, Gantt charts, pie charts, bar charts, and bubble charts					
8.11.13	Provide Red, Yellow, Green (RYG, AKA Red, Amber, Green RAG) project health indicators or similar on dashboards					
8.11.14	Track and report project pipeline, backlog, completed projects, etc.					
8.11.15	Report financial forecast and actuals by date range					
8.11.16	Report resource forecast and actuals by date range					
8.11.17	Report spending patterns across different types of projects					
8.11.18	Enable permissions to allow any user to create their own reports or views					
8.11.19	Capability to publish dashboards to be viewed by non-users of the system					
8.11.20	Automatically schedule the emailing of links to reports to non-users of the system on a daily, weekly, or monthly basis					
8.11.21	Filter data on user-definable criteria					
8.11.22	Produce ad hoc queries and reporting capability on-demand to include a view multi-year targets and a long range (21 year) financial plan derived from the strategic plan and provide a “roll up view” for annual reporting purposes. System must accomodate business processes for capturing all the project previous years expenditures, current year budget and expenditures, 5-year Capital Improvement Fund budget years 1 to 5 summary years and total of year 1 to 5, and the Long Range Financial Plan which includes years 6 through 20 as part of the budgeting process.					
8.11.23	Track project related key performance indicators (KPIs) and metrics such as Earned Value Analysis (EVA) to facilitate the tracking of project progress					
8.11.24	Generate, print, attach and forward compliance reporting templates and provide access to detailed report information through on screen report interactive drill-down from within reports					
8.11.25	Export all reports to Excel, PDF, PowerPoint and CSV format					
8.11.24	Option to develop up to five (5) custom reports/dashboards					
8.12	**Integrations**					
8.12.1	Web Services Application Program Interface (API)					
8.12.2	Custom integrations developed, hosted, and continually managed by vendor					

#	Compliance Matrix	Compliance	Proposer Questions	Capital Metro Response	Proposer Comments	Test #
8.12.3 Changed in Amendment 1	Provides and supports integration with Oracle Fusion Cloud Financials/HR test and production systems. As this PPM System goes live in October, 2022, the PPM System is expected to integrate with Oracle test systems and continue into user acceptance test as an integrated system with Oracle Cloud ERP. This PPM System is expected to go live in two phases with a probable update following the second go-live. I. The initial phase go-live by ~~July 1, 2022~~ October 3, 2022 will allow the system to perform the project proposal (Project Initiating) activities: (1) Project Proposals (2) Dependency Management (3) Portfolio Prioritization (4) Budget Requests and Review - in PPM System only, Oracle integration in (7) below II. The subsequent go-live in ~~October, 2022~~ January 2023 will provide: (5) Integrations with Oracle (6) Migration of EPPM Tool data to PPM System (7) Budget Requests and Review (Oracle Integration) (8) Project Planning Management (9) Project Executing Management (10) Project Monitoring & Controlling Management including Budget Change Requests (11) Project Closeout (12) Archiving The following are the integrations that are envisioned starting ~~October, 2022~~January 2023: (1) Ability to send Oracle Budgeting (EPM) new project requests along with EAC for budget planning and budget change requests. (2) Ability to send project meta data to Oracle PPM. (3) Ability to receive project resources from Oracle HR. (4) Ability to receive Oracle chart of accounts segments from Oracle GL. (5) Ability to receive budgets, (includes transfers, revised budgets) encumbrances, (commitments & obligations) actual expenditures, includes time and expenses from Oracle. The PPM System must integrate with Oracle (vendor) published rest APIs for the inbound and outbound integrations. III. Probable update for Oracle integration for HR data. It is assumed that the base resource data will already be included for the 1st Go-Live for the project proposal process, October 2022. An update may be needed for resource data when the Oracle HR module is fully live after March 2023.					
8.12.4	Import / export from MS Excel					
8.12.5	SAML 2.0 based Single Sign on capability					
8.12.6	MS Project or approved equivalent					
8.12.7 Changed in Amendment 1	The first go-live date of October 3, 2022 was selected to support the Capital Metro business process of beginning entry of project proposals for the following fiscal year in October because PMs need extended time to collaborate with stakeholders in developing the full-spectrum of project proposal requirements. This start date gives them about two full fiscal quarters to build the proposal which is needed because of our commitment to collaboration across the agency to reduce risks of exceeding capacity to deliver projects.					
8.13	**Security**					
8.13.1	Vendor shall secure all databases according to industry best practices and shall ensure that databases are not directly accessible to the internet.					
8.13.2	Vendor shall ensure that the hosted solution is segmented from their corporate network so that malware affecting the corporate network cannot affect the hosted environment and application.					
8.13.3	Vendor shall utilize application layer firewalls in addition to network layer firewall to protect the application and customer data.					
8.13.4	Vendor shall have detective controls to monitor and log database activity and shall have data loss prevention tools.					
8.13.5	ALL data such as passwords and credit card numbers shall be encrypted at rest and in transit.					
8.13.6	Vendor shall secure all databases according to industry best practices and shall ensure that databases are not directly accessible to the internet.					
8.13.7	Vendor shall ensure that the hosted solution is segmented from their corporate network so that malware affecting the corporate network cannot affect the hosted environment and application.					
8.13.8	Vendor shall utilize application layer firewalls in addition to network layer firewall to protect the application and customer data.					
8.13.9	Vendor shall have detective controls to monitor and log database activity and shall have data loss prevention tools.					

#	Compliance Matrix	Compliance	Proposer Questions	Capital Metro Response	Proposer Comments
3.0	**Phase Tasks and Deliverables.** The Contractor shall perform the following phase tasks and provide the associated deliverables required to deploy all software, updates and configurations resulting in a fully functional and tested system. Contractor shall obtain Capital Metro review of all deliverables and make changes and updates to deliverables per Capital Metro review as needed. Capital Metro acceptance of all deliverables for each phase as evidenced by a signed phase acceptance certificate is required prior to invoicing.				
3.1	**Plan.** Meet with Capital Metro project manager and business area stakeholders for project planning, including review of proposed schedule, roles and responsibilities, as well as conduct a complete review of functionality to be delivered, and other project activities. Plan Deliverables:				
3.1.1.	Project organization chart				
3.1.2	Project schedule (draft)				
3.1.3	Action Items and Issues log (AIL)				
3.1.4	Review and comment on Capital Metro Project Management Plan				
3.1.5	Infrastructure and Integration Audit				
3.1.6	Initiate Risk Register				
3.1.7	System Implementation Plan (draft)				
3.1.8	Compliance Matrix Review and Update				
3.1.9	Kick-off meeting and base product demo with stakeholders to review and clarify requirements including confirmation of any required updates to Capital Metro's environment regarding licensing, network infrastructure etc., identified in the proposal				
3.1.10	Notification of plan phase completion with proof of deliverables				
3.1.11	Sign off on plan phase acceptance certificate				
3.1.12	Phase invoice upon receipt of Capital Metro authorization to invoice				
3.2	**Design. Contractor's technical requirements gathering and detailed design, beginning with an assessment and discussion with affected Capital Metro departments. This phase will determine how the system will be configured, product Wireframes/GUI presentation to the customer, and how it will be managed in the back end. The Contractor will work with Capital Metro to develop materials that will provide a basis to help instruct Capital Metro stakeholders in the easiest and most efficient way to use the system to their utmost advantage. Design Deliverables:**				
3.2.1	Assessment; Documentation of Findings				
3.2.2	Configuration Management Document ("CMD" - Draft)				
3.2.3	Wireframes/GUI diagrams (Draft)				
3.2.4	System Implementation Plan (Final)				
3.2.5	Disaster Recovery Plan (Draft)				
3.2.6	Quality Assurance Plan (Draft)				
3.2.7	Risk Management Plan participation (Final)				
3.2.8	Installation Plan (Draft)				
3.2.9	Deinstallation Plan (Draft)				
3.2.10	Review of Design and System Implementation Plan with Stakeholders				
3.2.11	Change Recommendations for Capital Metro Business Process Flowcharts for PPM System Effectiveness				

#	Compliance Matrix	Compliance	Proposer Questions	Capital Metro Response	Proposer Comments
3.2.12	Update of Design based on review				
3.2.13	Project Schedule (Baseline) with Resource Loading				
3.2.14	Review and Acceptance of Capital Metro Project Management Plan				
3.2.15	Compliance Matrix Review and Update				
3.2.16	Notification of Design Phase Completion with Proof of Deliverables				
3.2.17	Sign off on Design Phase Acceptance Certificate				
3.2.18	Phase Invoice upon Receipt of Capital Metro Authorization to Invoice				
3.3	**Develop.** Development, configuration and installation of the solution and integration as well as installation within a development and a test environment so configuration and testing of the required functionality can be started. This task will include setting the initial configuration values by the Contractor so they can be tested and changed if needed. During this phase, the rollout of the system must be worked on to include training all IT and Operational staff who will use or have on-going support roles. Develop Deliverables:				
3.3.1	Quality Assurance Plan Including QA/QC Checklist (Final)				
3.3.2	Development Environment Installation				
3.3.3	Test Environment Installation				
3.3.4	Supporting Infrastructure Implemented				
3.3.5	Application and Functionality Development				
3.3.6	Test Procedure/Plan including Test Scripts, Use Cases, Acceptance Test Criteria Demonstrating that Each Component of the Compliance Matrix is Developed and Meets Requirement (Draft)				
3.3.7	Update Compliance Matrix with Test Number(s)				
3.3.8	CMD Values Test and Update				
3.3.9	Review of Capital Metro Changes to Business Process Flowcharts				
3.3.10	High-level Training of Capital Metro Staff to Prepare for Test Phase				
3.3.11	Role-based Training Plan for all User Types (Draft)				
3.3.11.1	Submit a training plan including the training schedule and course outlines for review a minimum of three weeks prior to the scheduled classes				
3.3.11.2	The training shall be based on roles so that there are separate training sessions for project managers, resource managers, SMEs, and steering committee comprised of executive staff or those with other oversight responsibilities				
3.3.11.3	Arrange for an instructor(s) with thorough knowledge of the material covered in the course(s) and the ability to effectively lead the knowledge transfer				
3.3.11.4	Provide customized training manuals specific to Capital Metro's environment in Microsoft Word and PDF. Contractor shall provide hard copies in the number of agreed-to number of training participants as well as the Instructor versions				
3.3.12	Warranty and Maintenance Plan Review				
3.3.13	Review and Feedback of Capital Metro Support Responsibility Matrix				
3.3.14	Notification of Develop Phase Completion with Proof of Deliverables				
3.3.15	Sign off on Develop Phase Acceptance Certificate				
3.3.16	Phase Invoice upon Receipt of Capital Metro Authorization to Invoice				

#	Compliance Matrix	Compliance	Proposer Questions	Capital Metro Response	Proposer Comments
3.4	Test. Integration and testing by Contractor and Capital Metro to determine that all functionality required of the installed PPM System, software, hand-held validators, off board validators and integrations into the existing environment is in place and working. The testing phase shall not be deemed complete until all functional requirements of the newly implemented system have been fully tested and approved by the project team. The Contractor shall provide a Test Procedure document with test scripts, use cases and acceptance test criteria for review and acceptance by Capital Metro for all phases. Only Capital Metro data is to be used for testing. Before Capital Metro performs any testing, the Contractor shall provide the written test results of the full test procedure/plan demonstrating no Class 1 or Class 2 failures. Test Deliverables:				
3.4.1	Activation of any required licenses				
3.4.2	Training Plan (Final)				
3.4.3	Document Procedures and Migrate Environment from Development to Test				
3.4.4	Contractor's Successfully Test Procedure/Plan Results				
3.4.5	Documentation including User and Training Manuals (Draft)				
3.4.6	Test Procedure/Plan including Test Scripts, Use Cases and Acceptance Test Criteria (Final)				
3.4.7	System Acceptance Test (SAT) Plan Developed (Subset to Use to Determine Go, No-Go before Go Live)				
3.4.8	Security Penetration Test				
3.4.9	Disaster Recovery Test – End-to-End				
3.4.10	Test Failure Log & Remediation Plan. Contractor shall lead testing of the solution including integrations and resolve all Significant (Class 1) and Severe (Class 2) Test Failure Results (TFRs). Contractor shall endeavor to resolve Minor (Class 3) TFRs during this phase; however, the requirement for Class 3 resolution is during the Closeout phase. Definition for each class are as follows:				
	Severe - A Class 1 test failure is a severe defect that prevents, inhibits, or significantly impairs further testing or operation of the system				
	Significant - A Class 2 test failure is a significant defect that does not prevent further testing or has a minimal effect on normal operations of the system				
	Minor – A Class 3 test failure is a minor or isolated defect that does not impact or invalidate the testing or normal operations of the system				
3.4.11	Regression Testing of the Entire Test Plan for any Class 1 and Class 2 Failures				
3.4.12	Introduction to Contractor's Support Manager and Team				
3.4.13	Detailed Processes and Contact Information for Post Go Live Support				
3.4.14	Compliance Matrix Review and Update				
3.4.15	Notification of Test Phase Completion with Proof of Deliverables				
3.4.16	Sign off on Test Phase Acceptance Certificate				
3.4.17	Phase Invoice upon Receipt of Capital Metro Authorization to Invoice				

#	Compliance Matrix	Compliance	Proposer Questions	Capital Metro Response	Proposer Comments
3.5	**Deploy/Go Live.** Deploy: once all the test failures have been corrected, the Contractor shall install and configure the software and incorporate it into the live environment. Go Live: the system shall go live and be monitored for the first 30 days of operation. If Severe (Class 1) or Significant (Class 2) issues arise, the Go-Live period may be cancelled, extended or restarted. The Contractor shall be required to participate in the monitoring of the system and respond to issues so they are quickly resolved. Deploy/Go Live Deliverables:				
3.5.1	Conduct Training for all User Types				
3.5.2	Document Procedures and Migrate Environment from Test to Production				
3.5.3	QA/QC checklist Sign off				
3.5.4	Delivery and Inventory of Spares (e.g. optional hand-held devices)				
3.5.5	Update to Disaster Recovery Plan				
3.5.6	Delivery of all Documentation including User and Training Manuals (Revise Draft)				
3.5.7	Deployment, Implementation, Configuration and Integration the PPM System with all environments				
3.5.8	Migration of Capital Metro historical data				
3.5.9	During contract period, Contractor shall provide a storage container for equipment storage and Capital Metro will provide space for container				
3.5.10	System Acceptance Test (SAT)				
3.5.11	Resolution of SAT TFRs				
3.5.12	Go Live Schedule and Transition Plan				
3.5.13	System Go Live				
3.5.14	Technical Lead on-site During First Week of Go Live, or Longer if System Issues are Experienced				
3.5.15	Review and coordinate with Capital Metro to update Capital Metro Business Process Flowcharts for PPM System effectiveness				
3.5.16	Revised (final) Copies of all Required Documentation including User and Training Manuals				
3.5.17	Compliance Matrix Review and Update				
3.5.18	Notification of Plan Phase Completion with Proof of Deliverables				
3.5.19	Sign off on Go Live Phase Acceptance Certificate				
3.5.20	Phase Invoice upon Receipt of Capital Metro Authorization to Invoice				
3.6	**Close.** Obtain acceptance by Capital Metro to formally close the project. Apply appropriate updates to project documents. Close out all procurement activities ensuring termination of all relevant agreements. Close Deliverables:				
3.6.1	Follow-up training on areas identified during Go Live and Training Documentation (Final)				
3.6.2	Final recommendations for Capital Metro-updated Process Flowcharts				
3.6.3	All AIL items closed				
3.6.4	Resolution of all Minor (Class 3) TFRs				
3.6.5	Final Documentation for Environment Refresh (Develop-Test-Production)				
3.6.6	Disaster Recovery Plan (Final)				
3.6.7	Configuration Management Documents (CMD – Final)				
3.6.8	APIs and All Documentation Related to All Integrations (Final)				
3.6.9	Warranty and Maintenance Procedure Review and Forms				
3.6.10	As-builts: updates to any documentation including design document changes				

#	Compliance Matrix	Compliance	Proposer Questions	Capital Metro Response	Proposer Comments
3.6.11	Participation in Lessons Learned				
3.6.12	Notification of Closeout Phase Completion with Proof of Deliverables				
3.6.13	Sign off on Closeout Acceptance Certificate				
3.6.14	Final Invoice upon Receipt of Capital Metro Authorization to Invoice				
4.0	**Project Management.** The Contractor shall manage the project continuously beginning with the Notice to Proceed through Close, and shall lead the project and is expected to drive and manage all aspects of the project including the management of any subcontractors. Capital Metro shall manage and coordinate all its resources. A PMP is preferred and shall be approved by Capital Metro. Project Management Deliverables:				
4.1	Active Partnership with Capital Metro in assuring Project Success				
4.2	Single Point of Contact for All Communication Regarding Work Under This Contract				
4.3	Task Coordination with The Designated Capital Metro project manager				
4.4	Regular Communication with The Project Manager and any other staff designated to discuss progress, critical risk factors, schedule, or unique issues that may surface				
4.5	Specification of Capital Metro's staff resources needed for project success with at least two weeks notice in advance within the project schedule				
4.6	Support Responsibility Matrix Review and Updates as Needed				
4.7	Semi-monthly Status Meetings with Updated Schedule and AIL				
4.8	Review and Feedback of Change Requests as Needed				
4.9	Monthly Risk Registry Updates				
4.10	Monthly Management Review Meetings				
4.11	Monthly Project Status Report				
4.12	Quarterly attendance and Status Presentation at Steering Committee Meetings				
4.13	Responsible for ensuring all project documentation, including meeting minutes, AIL updates, project schedule and plans are kept updated in the Capital Metro SharePoint site				
5.0	**Payment Milestones.** Payment for each of the above described project phases shall be paid in the following percentages of total Project Costs. Should Contractor propose different or additional milestones, Capital Metro will review as submitted.				
5.1	Plan: 10%				
5.2	Design: 15%				
5.3	Develop: 15%				
5.4	Test: 15%				
5.5	Deploy/Go Live: 30%				
5.6	Closeout: 15%				
6.0	**Payment Method.** Payment will be governed based on:				
6.1	Notification of Phase Completion with Proof of Deliverables				
6.2	Sign off on Capital Metro's Phase Acceptance Certificate by Contractor's representatives and Capital Metro project team and/or project Executive Stakeholders				
6.3	Phase Invoice upon Receipt of Capital Metro Authorization to Invoice which must contain the Capital Metro signed Acceptance Certificate and the Capital Metro Purchase Order number				

#	Compliance Matrix	Compliance	Proposer Questions	Capital Metro Response	Proposer Comments
7.0	Contract Completion/Termination. Within five (5) days of the expiration or termination of a final agreement for any reason, or upon Capital Metro's request, Contractor will provide Capital Metro with a copy of all relevant portions of Capital Metro data, without limitation, from the PPM System and associated servers or other storage means and assist with and accommodate transition/transfer of such data to Capital Metro or another provider. The format of the data transition shall be determined by Capital Metro.				

Control Group	Control Heading	Original ID	Control Specification	Assessment Questions	Answer	Notes/Comment
Application & Interface Security	**Application Security**	AIS-01.2	Applications and programming interfaces (APIs) shall be designed, developed, deployed and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Do you use an automated source code analysis tool to detect security defects in code prior to production?		
		AIS-01.5		(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?		
	Customer Access Requirements	AIS-02.1	Prior to granting customers access to data, assets, and information systems, (removed all) identified security, contractual, and regulatory requirements for customer access shall be addressed.	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?		
				Does the application support role based data access control?		
	Data Integrity	AIS-03.1	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	Does your data management policies and procedures require audits to verify data input and output integrity routines?		
	Data Security / Integrity	AIS-04.1	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity and availability) across multiple system interfaces, jurisdictions and business functions to prevent improper disclosure, alternation, or destruction.	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS, PCI)? Specify the standards that you use.		
				Is customer data ever shared with or is visible to 3rd party vendors?		
				Does customer data ever leave the hosted environment?		
				Is the application PCI compliant?		
				Are credit card numbers masked to show only the last 4 digits?		
Audit Assurance & Compliance	**Independent Audits**	AAC-02.1	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures and compliance obligations.	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?		
		AAC-02.2		Do you conduct network penetration tests of your cloud service infrastructure at least annually?		
		AAC-02.3		Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?		
	Information System Regulatory Mapping	AAC-03.1	Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?		
		AAC-03.3		Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?		
		AAC-03.4		Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?		

Control Group	Control Heading	Original ID	Control Specification	Assessment Questions	Answer	Notes/Comment
Business Continuity Management & Operational Resilience	**Business Continuity Testing**	BCR-02.1	Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?		
	Impact Analysis	BCR-9.3	There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following: • Identify critical products and services • Identify all dependencies, including processes, applications, business partners, and third party service providers • Understand threats to critical products and services • Determine impacts resulting from planned or unplanned disruptions and how these vary over time • Establish the maximum tolerable period for disruption • Establish priorities for recovery • Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption • Estimate the resources required for resumption	Do you provide customers with ongoing visibility and reporting of your SLA performance?		
	Policy	BCR-10.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?		
	Retention Policy	BCR-11.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.	Do you have technical capabilities to enforce tenant data retention policies?		
		BCR-11.3		Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?		
		BCR-11.7		Do you test your backup or redundancy mechanisms at least annually?		
Change Control & Configuration Management	**Outsourced Development**	CCC-02.1	External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g. ITIL service management processes).	Do you have controls in place to ensure that standards of quality are being met for all software development?		

Control Group	Control Heading	Original ID	Control Specification	Assessment Questions	Answer	Notes/Comment
		CCC-02.2		Do you have controls in place to detect source code security defects for any outsourced software development activities?		
	Management Quality Testing	CCC-03.3	Organization shall follow a defined qualty change control and testing process (e.g. ITIL Service Management) with established baselines, testing and release standards which focus on system availability, confidentiality and integrity of systems and services	Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?		
		CCC-03.4		Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?		
	Unauthorized Software Installations	CCC-04.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?		
Data Security & Information Lifecycle Management	**Classifications, eCommerce Transactions, Data Inventory / Flows**	DSI-01.3	Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.	Do you have a capability to use system geographic location as an authentication factor?		
		DSI-01.5		Can you provide the physical location/geography of storage of a tenant's data in advance?		
		DSI-02.1	Policies and procedures shall be established to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's applications and infrastructure network and systems. In particular, providers shall ensure that data that is subject to geographic residency requirements not be migrated beyond its defined bounds.	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?		
		DSI-03.1	Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.	Do you provide standardized (e.g. ISO/IEC) non-proprietary encryption algorithms (3DES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?		
		DSI-03.2		Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?		
	Nonproduction Data	DSI-05.1	Production data shall not be replicated or used in non-production environments.	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?		
	Secure Disposal	DSI-07.1	Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.	Do you support the secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data?		
		DSI-07.2		Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?		

Control Group	Control Heading	Original ID	Control Specification	Assessment Questions	Answer	Notes/Comment
Datacenter Security	**Asset Management**	DCS-01.1	Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership y defined roles and responsibilities.	Do you maintain a complete inventory of all of your critical assets located at all sites/ or geographical locations and their assigned ownership?		
	Controlled Access Points	DCS-02.1	Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented for all areas housing sensitive data and information systems?		
	User Access	DCS-09.1	Physical access to information assets and functions by users and support personnel shall be restricted.	Do you restrict physical access to information assets and functions by users and support personnel?		
				Does all remote access require 2 Factor authentication?		
Encryption & Key Management				What is the encryption methodology and ciphers used to protect the data?		
	Key Generation	EKM-02.1	Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.	Do you have a capability to allow creation of unique encryption keys per tenant?		
		EKM-02.3		Do you maintain key management procedures?		
	Encryption	EKM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.	Do you encrypt tenant data at rest (on disk/storage) within your environment?		
		EKM-03.4		Do you have documentation establishing and defining your encryption management policies, procedures and guidelines?		

Control Group	Control Heading	Original ID	Control Specification	Assessment Questions	Answer	Notes/Comment
Governance and Risk Management	**Baseline Requirements**	GRM-01.1	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and established and authorized based on business need.	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?		
		GRM-04.1	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business: • Risk management • Security policy • Organization of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information systems acquisition, development, and maintenance	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?		
	Policy	GRM-06.1	Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.	Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/function and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)?		
	Policy Enforcement	GRM-07.1	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?		

Control Group	Control Heading	Original ID	Control Specification	Assessment Questions	Answer	Notes/Comment
	Policy Reviews	GRM-09.1	The organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.	Do you notify your tenants when you make material changes to your information security and/or privacy policies?		
		GRM-09.2		Do you perform, at minimum, annual reviews to your privacy and security policies?		
Human Resources	**Asset Returns**	HRS-01.1	Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.	Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-owned assets?		
	Background Screening	HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?		
	Employment Agreements	HRS-03.1	Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.	Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies?		
				Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?		
		HRS-03.3		Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?		
	Employment Termination	HRS-04.1	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.	Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?		
	Training / Awareness	HRS-09.5	A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	Are personnel trained and provided with awareness programs at least once a year?		
Identity & Access Management	**Audit Tools Access**	IAM-01.1	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?		
		IAM-01.2		Do you monitor and log privileged access (e.g., administrator level) to information security management systems?		

Control Group	Control Heading	Original ID	Control Specification	Assessment Questions	Answer	Notes/Comment
	User Access Policy	IAM-02.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following: • Procedures and supporting roles and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships) • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems) • Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant)) • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?		
	Diagnostic / Configuration Ports Access	IAM-03.1	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	Do you use dedicated secure networks to provide management access to your cloud service infrastructure?		
	Policies and Procedures	IAM-04.1	Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?		
	Source Code Access Restriction	IAM-06.1	Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?		
		IAM-06.2		Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?		

Control Group	Control Heading	Original ID	Control Specification	Assessment Questions	Answer	Notes/Comment
	Third Party Access	IAM-07.7	The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.	Do you share your business continuity and redundancy plans with your tenants?		
		IAM-08.1	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.	Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege?		
	User Access Reviews	IAM-10.1	User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures.	Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (exclusive of users maintained by your tenants), based on the rule of least privilege, by business leadership or other accountable business role or function?		
	User Access Revocation	IAM-11.1	Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?		
	User ID Credentials	IAM-12.1	Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures: • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?		
		IAM-12.3		Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?		

Control Group	Control Heading	Original ID	Control Specification	Assessment Questions	Answer	Notes/Comment
		IAM-12.8		Do you support password (minimum length, age, history, complexity) and account lockout (lockout threshold, lockout duration) policy enforcement?		
		IAM-12.11		Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?		
Infrastructure & Virtualization Security	**Audit Logging / Intrusion Detection**	IVS-01.1	Higher levels of assurance are required for protection, retention, and lifecyle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?		
		IVS-01.2		Is physical and logical user access to audit logs restricted to authorized personnel?		
		IVS-01.5		Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?		
	Clock Synchronization	IVS-03.1	A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?		
	OS Hardening and Base Controls	IVS-07.1	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?		
	Production / Non-Production Environments	IVS-08.1	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?		
		IVS-08.3		Do you logically and physically segregate production and non-production environments?		
	Segmentation	IVS-09.1	Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations: • Established policies and procedures • Isolation of business critical assets and/or sensitive user data and sessions that mandate stronger internal controls and high levels of assurance • Compliance with legal, statutory and regulatory compliance obligations	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?		

Control Group	Control Heading	Original ID	Control Specification	Assessment Questions	Answer	Notes/Comment
	VMM Security - Hypervisor Hardening	IVS-11.1	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?		
	Wireless Security	IVS-12.1		Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?		
		IVS-12.2		Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings)?		
		IVS-12.3		Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?		
Interoperability & Portability	**APIs**	IPY-01.1	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?		
	Standardized Network Protocols	IPY-04.1	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.	Can data import, data export and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?		
Mobile Security	**Approved Applications**	MOS-03.1	The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device?		
	Awareness and Training	MOS-05	The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program.	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?		
Security Incident Management, E-Discovery, & Cloud Forensics	**Incident Management**	SEF-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.	Do you have a documented security incident response plan?		
				Do you have a dedicated security team?		
		SEF-02.4		Have you tested your security incident response plans in the last year?		

Control Group	Control Heading	Original ID	Control Specification	Assessment Questions	Answer	Notes/Comment
	Incident Reporting	SEF-03.1	Workforce personnel and external business relationships shall be informed of their responsibility and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.	Are workforce personnel and external business relationships adequately informed of their responsibility, and, if required, consent and/or contractually required to report all information security events in a timely manner?		
				What is your SLA for security incident notification?		
		SEF-03.2		Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations?		
				Does your logging and monitoring framework allow isolation of an incident to specific tenants?		
	Incident Response Legal Preparation	SEF-04.2	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?		
		SEF-04.3		Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?		
		SEF-04.4		Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?		
				Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?		
Supply Chain Management, Transparency, and Accountability	**Data Quality and Integrity**	STA-01.2	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.	Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?		
	Incident Reporting	STA-02.1	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g. portals).	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?		
	Network / Infrastructure Services	STA-03.1	Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.	Do you collect capacity and use data for all relevant components of your cloud service offering?		

Control Group	Control Heading	Original ID	Control Specification	Assessment Questions	Answer	Notes/Comment
	Third Party Agreements	STA-05.4	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations) • Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships • Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts • Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain) • Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed • Expiration of the business relationship and treatment of customer (tenant) data impacted	Do third-party agreements include provision for the security and protection of information and assets?		
		STA-05.5		Do you have the capability to recover data for a specific customer in the case of a failure or data loss?		
	Supply Chain Metrics	STA-07.4	Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall performed at least annually and identity non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?		

Control Group	Control Heading	Original ID	Control Specification	Assessment Questions	Answer	Notes/Comment
	Third Party Audits	STA-09.1	Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.	Do you mandate annual information security reviews and audits of your third party providers to ensure that all agreed upon security requirements are met?		
		STA-09.2		Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?		
Threat and Vulnerability Management	**Antivirus / Malicious Software**	TVM-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your IT infrastructure network and systems components?		
	Vulnerability / Patch Management	TVM-02.1	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g. network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices? How often do you perfom vulnerability scans?		
				What is your security patch process and how often do you push updates?		
				Will the customers be impacted during updates and maintenace windows?		
				Do you have a process for notifying customers of updates and maintenance?		
		TVM-02.2		Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?		
		TVM-02.3		Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?		
		TVM-02.5		Do you have a capability to patch vulnerabilities across all of your computing devices, applications, and systems?		

Control Group	Control Heading	Original ID	Control Specification	Assessment Questions	Answer	Notes/Comment
	Mobile Code	TVM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?		