Responding Company, Inc.
123 Main Street
Great City, Colorado

# Service Provider RFP Technical Requirements

Approved April 17, 2017

RFP Title Here

RFP No. 1234A

***Our Vision***

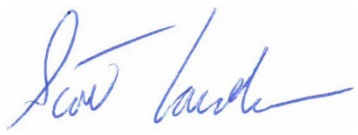
*Aspiring to be the nation's model for delivery of technology, media, and contact center services for local government.*

DENVER
TECHNOLOGY SERVICES

This page left intentionally left blank.

## Purpose

This Service Provider Request for Proposal (RFP) Technical Requirements document provides the basis for evaluating the information security maturity and compatibility of vendors providing cloud or hosted services.

| Approval |
| --- |
|  |
| Scott Cardenas, Chief Information Officer<br>Technology Services |
| Date: April 17, 2017 |

## General Instructions

We expect the selected vendor to operate as a mature IT organization according to best practices.

To complete the RFP requirements, the vendor must submit information for both sections outlined below:

1. Section I contains questions focused on the City and County of Denver, specifically to our environment and unique requirements.

2. Section II evaluates the technical maturity of our vendors using industry standards when regulatory data will be included in the project. Regulatory data include HIPAA, CJI, PCI, PII, etc.

## Completing Section I – Mandatory RFP Requirements

Regardless of the submission method used for Section II, all vendors must submit responses to the questions in Section I. All questions in this section are mandatory and must be answered to complete the RFP submission.

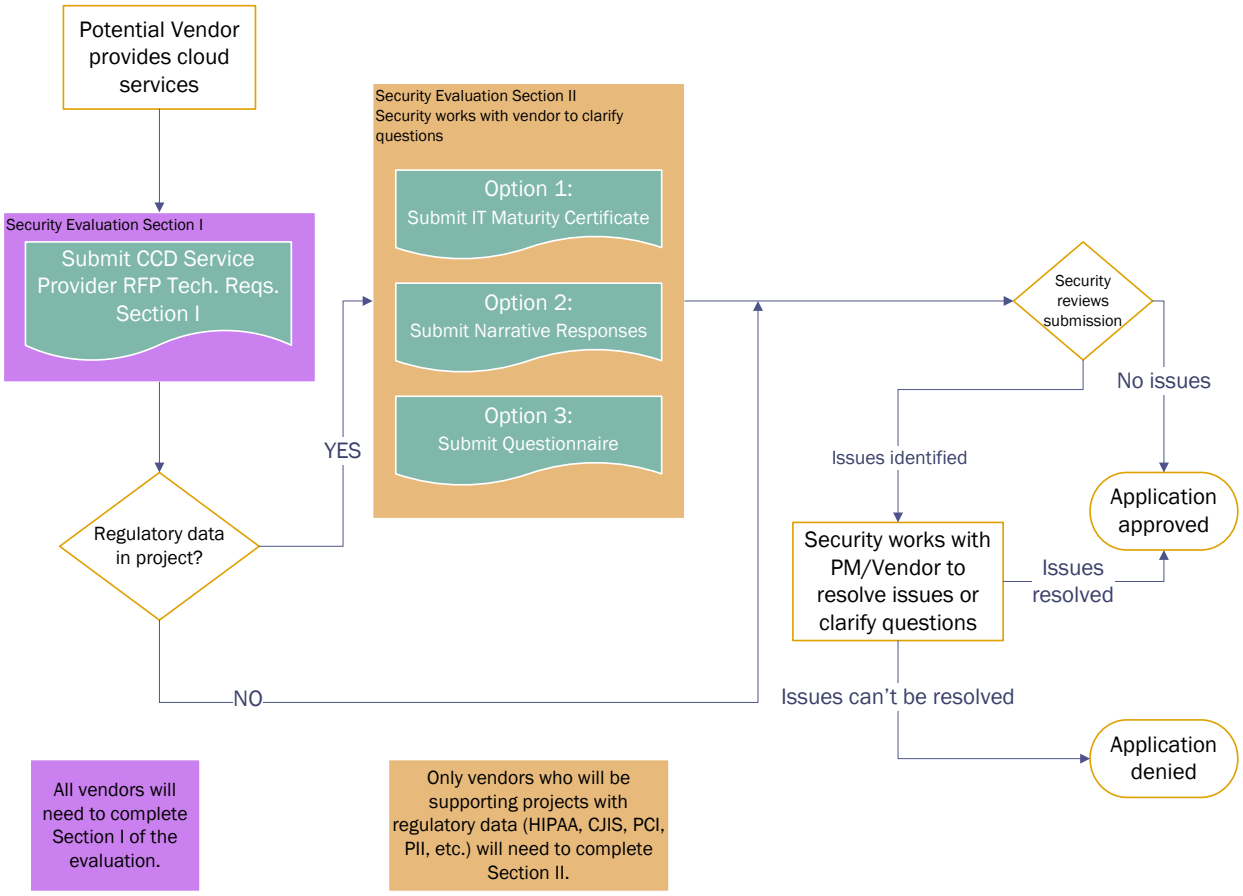
## Completing Section II – Technical Maturity

Section II is required when regulatory data is going to be included in the project. If regulatory data is not used, Section II is not required to be completed. One of the following options is required to complete the submission when regulatory data will be used in the project.

- Option 1 – Submit certificate of IT maturity
- Option 2 – Complete narrative questions
- Option 3 – Complete questionnaire

## Process Flow

The process pictured below shows the high level steps that are completed to approve the submitted proposal.



## Table of Contents

# Contents

# Section I – Mandatory RFP Requirements

If the cloud service being proposed does not meet the technical specifications provided in this section, proposals may be submitted; however, a technology exception waiver must be applied for and granted by the Technology Services Leadership Team as a term and condition of the contract. If future compliance is planned (*i.e.*, in a future release of the proposed software or system) please note that clearly in the waiver and in the proposal.

## 1. Identity Management

### 1-CCD-01 Oracle Identity Management

The City's Identity and Access Management (IdM) system is an integrated infrastructure solution that enables many of the City's services and online resources to operate more efficiently, effectively, economically and securely. All new and proposed applications must utilize the authentication and authorization functions and components of the IdM. Strong authentication is required for privileged accounts or accounts with access to sensitive information. This technical requirement applies to all solutions, regardless to where the application is hosted.

### 1-CCD-02 (re: IAM-12) User ID Credentials

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:

a) Identity trust verification and service-to-service application (API) and information processing interoperability (*e.g.*, SSO and Federation)
b) Account credential lifecycle management from instantiation through revocation
c) Account credential and/or identity store minimization or re-use when feasible
d) Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (*e.g.*, strong/multi-factor, expireable, non-shared authentication secrets)

## 1. Identity Management

Please provide a short narrative that describes the controls you have in place for the requirements listed above. Consult the detailed controls to help clarify the topic. You are required to directly answer each of the detailed controls. You may optionally provide documentation to support your answer in an appendix that you supply. We reserve the right to request documentation that substantiates your answers, such as, copies or examples of policy, examples of metrics, assessments, agreements, architectural or data flow diagrams, reports of compliance, etc.

# 2. End-User Device Compatibility

### 2-CCD-01 City Client Device Compatibility

A city client device refers to the computing equipment used by City and County of Denver employees, officers or personnel working on behalf of the City and County of Denver. At the present time, these devices incorporate desktops, laptop and tablets. If the cloud service solution being proffered is highly dependent or tightly coupled with hardware specifications or installed software (*e.g.*, Java JRE version) please consult with the City's Purchasing office for the current deployed environment in the agency, department, or area of interest.

### Desktop, Workstation, and Laptop Hardware

The cloud solution being acquired must be compatible with the current desktop, laptop, or tablet computing environment. The specifications are based on the City's hardware lifecycle bid process and represent the expected maximum hardware specification for that class of hardware. Currently, there are two active bid cycles, 2007 and 2013. Both hardware bid cycles have been included to serve as reference for current and future hardware environment state.

| Bid | 2007 - 2013 | | | | 2013 – 2018+ | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Hardware Class | Basic PC | Advanced PC | Workstation PC | Standard Laptop | Basic PC | Advanced PC | Workstation PC | Standard Laptop | Ultrabook | Workstation Laptop | Tablet |
| Intel E2140, 1.6GHz | • | | | | | | | | | | |
| Intel Xeon 5130, 2.0 GHz | | • | | | | | | | | | |
| Intel Dual-Core Xeon 5160, 3.0 GHz | | | • | | | | | | | | |
| Intel Core 2 Duo T7100, 1.8 GHz | | | | • | | | | | | | |
| Intel Quad-Core i5-3470, 3.2 GHz | | | | | • | | | | | | |
| Intel Quad-Core i7-3770, 3.4 GHz | | | | | | • | | | | | |
| Intel 6-Core Xeon E6-2630, 2.3 GHz | | | | | | | • | | | | |
| Intel Dual-Core i5-3360M, 2.8 GHz | | | | | | | | • | | | |
| Intel Dual-Core i7-3667U, 2.0 GHz | | | | | | | | | • | | |
| Intel Quad-Core i7-374-QM, 2.7GHz | | | | | | | | | | • | |
| Intel Atom Z2760, 1.8 GHz | | | | | | | | | | | • |
| RAM (GB) | 2 | 2 | 4 | 2 | 4 | 4 | 16 | 4 | 8 | 8 | 2 |
| ATI Radeon X300 | • | | | | | | | | | | |
| nVidea Quadro FX 3450, 256 MB | | • | • | | | | | | | | |
| Intel X3100 Integrated | | | | • | | | | | | | |
| Radeon HD7470, 1GB | | | | | • | | | | | | |
| Radeon HD7570, 1GB | | | | | | • | | | | | |
| nVidea Quadro 4000, 2GB | | | | | | | • | | | | |
| Intel HD Graphics 400 | | | | | | | | | • | | |
| AMD FirePro M4000 1GB | | | | | | | | | | • | |

### Software

The City and County of Denver installs and maintains standard software on all desktops and laptops. All software that is acquired by the City and County of Denver must be compatible with the expected environment and previous versions of the following software products.

| Software Type | Software Name | Technical Requirement |
|---|---|---|
| Operating System | Microsoft Windows | Win 7 Professional SP1 64-bit; Win 10 Version 1511 and above |

| Software Type | Software Name | Technical Requirement |
|---|---|---|
| Browsers | Internet Explorer | Current Release |
| | Google Chrome | Latest Version |
| Office Suite | Microsoft Office | 0365 Office 2016 |
| Software Framework | Microsoft .NET | 4.0 |
| Java | JRE | Current Release |
| Adobe | Acrobat Reader | Current Release |
| | Flash Player | Current Release |
| | Shockwave | Current Release |
| External Drives | McAfee Encryption | Current Release |
| Multimedia Framework | HTML 5 | Current Release |

**Mobile Devices**

The City and County of Denver supports the following mobile devices. Any software that is intended to run on mobile devices should support the following specifications.

| Device | Technical Requirement |
|---|---|
| iPhone | Current Release |
| iPad | |
| Android | |
| Windows Phone | |

**2-CCD-02 Public Client Device Compatibility**

A client device for public users refers to the computing equipment used by the public.

### Web Browsers

All web applications acquired by the City and County of Denver that will be accessed by the public must be compatible with the following web browser versions:

| Software Type | Software Name | Technical Requirement |
|---|---|---|
| Browsers | Internet Explorer | Current Version |
| | Google Chrome | |

## 2. End-User Device Compatibility

Please provide a short narrative that describes the controls you have in place for the City and County of Denver control domain listed above. Consult the detailed controls to help clarify the topic. You do not need to directly answer each of the detailed controls; however, your answer must allow us to gain a thorough understanding of your control environment for the domain. You may optionally provide documentation to support your answer in an appendix that you supply. We reserve the right to request documentation that substantiates your answers, such as, copies or examples of policy, examples of metrics, assessments, agreements, architectural or data flow diagrams, reports of compliance, etc.

# 3. Statement of Network Impact

**3-CCD-01 Network Impact and Internet Traffic Shaping**

The City's network bandwidth is an expensive resource that is being shared among many City agencies and departments, and some applications require guaranteed bandwidth and priority. The City utilizes traffic shaping (*i.e.*, bandwidth shaping or packet shaping) as a general network control to prioritize and provide quality assurance to internet resources and guarantee certain bandwidth based on predefined policy rules.

The City recognizes that the cloud service user experience depends on many factors and that to quantify those factors is a difficult and arduous task. Therefore, the City has developed four (4) general traffic shaping policies available for new cloud services:

a) 500 kbps
b) 1 Mbps
c) 2 Mbps
d) 4 Mbps
e) Technology Waiver Request for Additional Shaping Policy

Based upon the cloud service offered, business requirements listed, number of expected concurrent clients, and other/additional knowledge of the service or services being offered within this RFP, choose a traffic shaping policy that maintains the user experience and provide a statement of network impact and justification that supports the policy requested, both quantitatively and qualitatively.

## 3. Statement of Network Impact

Please provide a short narrative that describes the controls you have in place for the City and County of Denver control domain listed above. Consult the detailed controls to help clarify the topic. You do not need to directly answer each of the detailed controls; however, your answer must allow us to gain a thorough understanding of your control environment for the domain. You may optionally provide documentation to support your answer in an appendix that you supply. We reserve the right to request documentation that substantiates your answers, such as, copies or examples of policy, examples of metrics, assessments, agreements, architectural or data flow diagrams, reports of compliance, etc.

# 4. Web Usability and Accessibility

**4-CCD-01 City and County of Denver URL Taxonomy**

All web pages and web application resources shall be served through the City's exclusive public domain (*i.e.*, "denvergov.org") or a City approved sub-domain (*e.g.*, "cloudservice.denvergov.org") thereof. The City and County of Denver requires all URLs and application URIs to be REST-ful utilizing best-practices. If clarification is necessary, contact the City for technical specification

**4-CCD-02 Responsive Design and User Interface Compatibility**

The City expects the selected vendor to possess and continually develop a mature, responsive, accessible and consistent desktop, mobile, and tablet user interface. The City utilizes a responsive design framework for its "denvergov.org" domain.

**4-CCD-03 City and County of Denver Branding Standards**

The City expects the selected vendor to possess a consistent "look and feel" throughout the service that reflects the City's Intranet and/or Internet branding standards.

Note: Generic branding information may be found at http://www.denvergov.org/brandcenter.

## 4. Web Usability and Accessibility

Please provide a short narrative that describes the controls you have in place for the City and County of Denver control domain listed above. Consult the detailed controls to help clarify the topic. You do not need to directly answer each of the detailed controls; however, your answer must allow us to gain a thorough understanding of your control environment for the domain. You may optionally provide documentation to support your answer in an appendix that you supply. We reserve the right to request documentation that substantiates your answers, such as, copies or examples of policy, examples of metrics, assessments, agreements, architectural or data flow diagrams, reports of compliance, etc.

# 5. Systems Integrations

### 5-CCD-01 Oracle Enterprise Service Architecture (ESB or SOA)

The City's implementation of the Oracle Enterprise Service is an integrated infrastructure solution that enables many of the City's services and online resources to operate more efficiently, effectively, economically and securely. All new and proposed applications must utilize the service catalog, functions, and components of the ESB/SOA where appropriate. This technical requirement applies to all solutions, regardless to where the application is hosted.

### 5-CCD-02 Enterprise Cashiering

The City's implementation of Enterprise Cashiering Services is an integrated infrastructure solution that enables many of the City's cashiering services to operate more efficiently, effectively, economically and securely. All new and proposed applications must utilize the service, functions, and components of the Enterprise Cashiering system where appropriate. This technical requirement applies to all solutions, regardless to where the application is hosted. If selected, you should be advised that, in cases where the proposed solution has a cashiering function and the City and County of Denver Department of Finance determined that Enterprise Cashiering Services is not appropriate, you are still required to comply with the Department of Finance's Cash Handling Requirements.

### 5-CCD-03 Enterprise Document Management

The City's Enterprise Document Management (EDM) system is an integrated infrastructure solution that enables many of the City's services and online resources to store and retrieve documents of record efficiently, effectively, economically and securely. All new and proposed applications that generate documents of record must utilize the functions and components of the EDM.

### 5-CCD-04 Connections to External Systems and Integrated Systems

The provider shall specify how authentication and encryption will be handled for all external systems, such as databases, directories, and web services. All credentials required for communication with external systems shall be encrypted.

### 5-CCD-05 System and Application Logging

The City and provider shall specify what events are security-relevant and need to be logged, such as detected attacks, failed login attempts, and attempts to exceed authorization. The requirements shall also specify what information to log with each event, including time and date, event description, application details, and other information useful in forensic efforts. The City uses a centralized system for security information and event management. All new and proposed systems must utilize the centralized logging capability of this system. This technical requirement applies to all applications, regardless to where the solution is hosted.

## 5. Systems Integrations

Please provide a short narrative that describes the controls you have in place for the City and County of Denver control domain listed above. Consult the detailed controls to help clarify the topic. You do not need to directly answer each of the detailed controls; however, your answer must allow us to gain a thorough understanding of your control environment for the domain. You may optionally provide documentation to support your answer in an appendix that you supply. We reserve the right to request documentation that substantiates your answers, such as, copies or examples of policy, examples of metrics, assessments, agreements, architectural or data flow diagrams, reports of compliance, etc.

# 6. Disclosure of Datacenter Location(s)

**6-CCD-01 Physical Location of Datacenter(s)**

The provider shall disclose the physical location of all datacenters that may be utilized by the provider to host the services requested under this RFP. Disclosure shall include, but is not limited to: City and State (if located within the United States) or City, State equivalent and Country (if located outside the United States). If selected, the successful vendor should be advised a disclosure statement shall be an annual deliverable. Furthermore, disclosure is mandatory and required prior the provider hosting services requested under this RFP in a new or previously undisclosed datacenter.

## 6. Disclosure of Datacenter Location(s)

Please provide a short narrative that describes the controls you have in place for the City and County of Denver control domain listed above. Consult the detailed controls to help clarify the topic. You do not need to directly answer each of the detailed controls; however, your answer must allow us to gain a thorough understanding of your control environment for the domain. You may optionally provide documentation to support your answer in an appendix that you supply. We reserve the right to request documentation that substantiates your answers, such as, copies or examples of policy, examples of metrics, assessments, agreements, architectural or data flow diagrams, reports of compliance, etc.

# 7. Vendor Software

**7-CCD-01 Disclosure of Components**

The provider shall disclose all third-party software used in the development and execution or use of the software. Disclosure shall include, but is not limited to: all code libraries, frameworks, components, and other products (*e.g.*, Java JRE, .NET, jquery pluggins, etc.), whether commercial, free, open-source, or closed-source.

**7-CCD-02 Vendor Supported Releases**

The provider shall maintain the currency all third-party software used in the development and execution or use of the software including, but not limited to: all code libraries, frameworks, components, and other products (e.g., Java JRE, code signing certificates, .NET, jquery pluggins, etc…), whether commercial, free, open-source, or closed-source; with third-party vendor approved and supported releases.

## 7. Vendor Software

Please provide a short narrative that describes the controls you have in place for the City and County of Denver control domain listed above. Consult the detailed controls to help clarify the topic. You are required to directly answer each of the detailed controls. You may optionally provide documentation to support your answer in an appendix that you supply. We reserve the right to request documentation that substantiates your answers, such as, copies or examples of policy, examples of metrics, assessments, agreements, architectural or data flow diagrams, reports of compliance, etc.

# Section II. Technical Maturity

## Option 1 – IT Maturity Certificate

The vendor may have previously been certified by professional organizations that have the same technical requirements as City and County of Denver. Examples of certifications include: Service Organization Controls (SOC) 2, FedRAMP, Cloud Security Alliance Level 1, etc. The vendor may submit proof of current certification in lieu of completing Section II of this document.

## Option 2 – Narrative Responses

For each of the control domains please provide a short narrative that describes the controls you have in place. For your convenience and clarification, we have included all the detailed controls from the Cloud Security Matrix for each control domain. You do not need to directly answer each of the detailed controls, however, your answer must allow us to gain a thorough understanding of your control environment for each of the domains.

When answering the questions, you may optionally provide documentation to support your answer. We reserve the right to request documentation that substantiates your answers, such as: copies or examples of policy, examples of metrics, assessments, agreements, architectural or data flow diagrams, reports of compliance, etc.

# 8. Application and Interface Security

### 8-AIS-01 Application Security

Applications and interfaces (APIs) shall be designed, developed, and deployed in accordance with industry acceptable standards (*e.g.*, OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.

### 8-AIS-02 Customer Access Requirements

Prior to granting customers access to data, assets, and information systems, all identified security, contractual, and regulatory requirements for customer access shall be addressed and remediated.

### 8-AIS-03 Data Integrity

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.

### 8-AIS-04 Data Integrity and Security

Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure protection of confidentiality, integrity, and availability of data exchanged between one or more system interfaces, jurisdictions, or external business relationships to prevent improper disclosure, alteration, or destruction. These policies, procedures, processes, and measures shall be in accordance with known legal, statutory and regulatory compliance obligations.

## 8. Application and Interface Security

Please provide a short narrative that describes the controls you have in place for the Cloud Security Alliance Cloud Security Matrix control domain listed above. Consult the detailed controls to help clarify the topic. You do not need to directly answer each of the detailed controls; however, your answer must allow us to gain a thorough understanding of your control environment for the domain. You may optionally provide documentation to support your answer in an appendix that you supply. We reserve the right to request documentation that substantiates your answers, such as, copies or examples of policy, examples of metrics, assessments, agreements, architectural or data flow diagrams, reports of compliance, etc.

# 9. Audit Assurance and Compliance

### 9-AAC-01 Audit Planning

Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.

### 9-AAC-02 Independent Audits

Independent reviews and assessments shall be performed at least annually, or at planned intervals, to ensure that the organization addresses any nonconformities of established policies, procedures, and known contractual, statutory, or regulatory compliance obligations.

### 9-AAC-03 Information System Regulatory Mapping

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.

## 9. Audit Assurance and Compliance

Please provide a short narrative that describes the controls you have in place for the Cloud Security Alliance Cloud Security Matrix control domain listed above. Consult the detailed controls to help clarify the topic. You do not need to directly answer each of the detailed controls; however, your answer must allow us to gain a thorough understanding of your control environment for the domain. You may optionally provide documentation to support your answer in an appendix that you supply. We reserve the right to request documentation that substantiates your answers, such as, copies or examples of policy, examples of metrics, assessments, agreements, architectural or data flow diagrams, reports of compliance, etc.

# 10. Business Continuity Management and Operational Resilience

### 10-BCR-01 Business Continuity Planning

A consistent unified framework for business continuity planning and plan development shall be established, documented and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following:

a) Defined purpose and scope, aligned with relevant dependencies
b) Accessible to and understood by those who will use them
c) Owned by a named person(s) who is responsible for their review, update, and approval
d) Defined lines of communication, roles, and responsibilities
e) Detailed recovery procedures, manual work-around, and reference information
f) Method for plan invocation

### 10-BCR-02 Business Continuity Testing

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.

### 10-BCR-03 Datacenter Utilities and Environmental Conditions

Datacenter utilities services and environmental conditions (*e.g.*, water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.

### 10-BCR-04 Documentation

Information system documentation (*e.g.*, administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following:

a) Configuring, installing, and operating the information system
b) Effectively using the system's security features

### 10-BCR-05 Environmental Risks

Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.

### 10-BCR-06 Equipment Location

To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.

### 10-BCR-07 Equipment Maintenance

Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.

### 10-BCR-08 Equipment Power Failures

Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific business impact assessment.

### 10-BCR-09 Impact Analysis

There shall be a defined and documented method for determining the impact of any disruption to the organization that must incorporate the following:

a) Identify critical products and services
b) Identify all dependencies, including processes, applications, business partners, and third party service providers
c) Understand threats to critical products and services
d) Determine impacts resulting from planned or unplanned disruptions and how these vary over time
e) Establish the maximum tolerable period for disruption
f) Establish priorities for recovery
g) Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption
h) Estimate the resources required for resumption

### 10-BCR-10 Policy

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.

### 10-BCR-11 Retention Policy

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.

## 10. Business Continuity Management and Operational Resilience

Please provide a short narrative that describes the controls you have in place for the Cloud Security Alliance Cloud Security Matrix control domain listed above. Consult the detailed controls to help clarify the topic. You do not need to directly answer each of the detailed controls; however, your answer must allow us to gain a thorough understanding of your control environment for the domain. You may optionally provide documentation to support your answer in an appendix that you supply. We reserve the right to request documentation that substantiates your answers, such as, copies or examples of policy, examples of metrics, assessments, agreements, architectural or data flow diagrams, reports of compliance, etc.

# 11. Change Control and Configuration Management

### 11-CCC-01 New Development and Acquisition

Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and/or datacenter facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.

### 11-CCC-02 Outsourced Development

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).

### 11-CCC-03 Quality Testing

Organizations shall follow a defined quality 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.

### 11-CCC-04 Unauthorized Software Installations

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.

### 11-CCC-05 Production Changes

Policies and procedures shall be established for managing the risks associated with applying changes to:

a) Business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations.
b) Infrastructure network and systems components.

Technical measures shall be implemented to provide assurance that all changes directly correspond to a registered change request, business-critical or customer (tenant), and/or authorization by, the customer (tenant) as per agreement (SLA) prior to deployment.

## 11. Change Control and Configuration Management

Please provide a short narrative that describes the controls you have in place for the Cloud Security Alliance Cloud Security Matrix control domain listed above. Consult the detailed controls to help clarify the topic. You do not need to directly answer each of the detailed controls; however, your answer must allow us to gain a thorough understanding of your control environment for the domain. You may optionally provide documentation to support your answer in an appendix that you supply. We reserve the right to request documentation that substantiates your answers, such as, copies or examples of policy, examples of metrics, assessments, agreements, architectural or data flow diagrams, reports of compliance, etc.

## 12. Data Security and Information Lifecycle Management

**12-DSI-01 Classification**

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.

**12-DSI-02 Data Inventory and Flows**

Policies and procedures shall be established, and supporting business processes and technical measures implemented, to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's geographically distributed (physical and virtual) applications and infrastructure network and systems components and/or shared with other third parties to ascertain any regulatory, statutory, or supply chain agreement (SLA) compliance impact, and to address any other business risks associated with the data. Upon request, provider shall inform customer (tenant) of compliance impact and risk, especially if customer data is used as part of the services.

**12-DSI-03 eCommerce Transactions**

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.

**12-DSI-04 Data Handling and Labeling Security Policy**

Policies and procedures shall be established for labeling, handling, and the security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.

**12-DSI-05 Non-Production Data**

Production data shall not be replicated or used in non-production environments. 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.

**12-DSI-06 Ownership and Stewardship**

All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.

**12-DSI-07 Secure Disposal**

Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.

## 12. Data Security and Information Lifecycle Management

Please provide a short narrative that describes the controls you have in place for the Cloud Security Alliance Cloud Security Matrix control domain listed above. Consult the detailed controls to help clarify the topic. You do not need to directly answer each of the detailed controls; however, your answer must allow us to gain a thorough understanding of your control environment for the domain. You may optionally provide documentation to support your answer in an appendix that you supply. We reserve the right to request documentation that substantiates your answers, such as, copies or examples of policy, examples of metrics, assessments, agreements, architectural or data flow diagrams, reports of compliance, etc.

## 13. Datacenter Security

**13-DCS-01 Asset Management**
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 by defined roles and responsibilities.

**13-DCS-02 Controlled Access Points**
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.

**13-DCS-03 Equipment Identification**
Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.

**13-DCS-04 Off-Site Authorization**
Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premise.

**13-DCS-05 Off-Site Equipment**
Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premise. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full write of the drive to ensure that the erased drive is released to inventory for reuse and deployment or securely stored until it can be destroyed.

**13-DCS-06 Policy**
Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.

**13-DCS-07 Secure Area Authorization**
Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.

**13-DCS-08 Unauthorized Persons Entry**
Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.

**13-DCS-09 User Access**
Physical access to information assets and functions by users and support personnel shall be restricted.

## 13. Datacenter Security

Please provide a short narrative that describes the controls you have in place for the Cloud Security Alliance Cloud Security Matrix control domain listed above. Consult the detailed controls to help clarify the topic. You do not need to directly answer each of the detailed controls; however, your answer must allow us to gain a thorough understanding of your control environment for the domain. You may optionally provide documentation to support your answer in an appendix that you supply. We reserve the right to request documentation that substantiates your answers, such as, copies or examples of policy, examples of metrics, assessments, agreements, architectural or data flow diagrams, reports of compliance, etc.

## 14. Encryption and Key Management

### 14-EKM-01 Entitlement

Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.

### 14-EKM-02 Key Generation

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.

### 14-EKM-03 Encryption

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.

### 14-EKM-04 Storage and Access

Platform and data appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.

## 14. Encryption and Key Management

Please provide a short narrative that describes the controls you have in place for the Cloud Security Alliance Cloud Security Matrix control domain listed above. Consult the detailed controls to help clarify the topic. You do not need to directly answer each of the detailed controls; however, your answer must allow us to gain a thorough understanding of your control environment for the domain. You may optionally provide documentation to support your answer in an appendix that you supply. We reserve the right to request documentation that substantiates your answers, such as, copies or examples of policy, examples of metrics, assessments, agreements, architectural or data flow diagrams, reports of compliance, etc.

# 15. Governance and Risk Management

### 15-GRM-01 Baseline Requirements

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 authorized based on business needs.

### 15-GRM-02 Risk Assessments

Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following:

a) Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure
b) Compliance with defined retention periods and end-of-life disposal requirements
c) Data classification and protection from unauthorized use, access, loss, destruction, and falsification

### 15-GRM-03 Management Oversight

Managers are responsible for maintaining awareness of, and complying with, security policies, procedures and standards that are relevant to their area of responsibility.

### 15-GRM-04 Management Program

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:

a) Risk management
b) Security policy
c) Organization of information security
d) Asset management
e) Human resources security
f) Physical and environmental security
g) Communications and operations management
h) Access control
i) Information systems acquisition, development, and maintenance

### 15-GRM-05 Management Support and Involvement

Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.

**15-GRM-06 Policy**

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.

**15-GRM-07 Policy Enforcement**

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.

**15-GRM-08 Business & Policy Change Impacts**

Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.

**15-GRM-09 Policy Reviews**

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.

**15-GRM-10 Assessments**

Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (*e.g.*, audit results, threat and vulnerability analysis, and regulatory compliance).

**15-GRM-11 Program**

Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and stakeholder approval.

## 15. Governance and Risk Management

Please provide a short narrative that describes the controls you have in place for the Cloud Security Alliance Cloud Security Matrix control domain listed above. Consult the detailed controls to help clarify the topic. You do not need to directly answer each of the detailed controls; however, your answer must allow us to gain a thorough understanding of your control environment for the domain. You may optionally provide documentation to support your answer in an appendix that you supply. We reserve the right to request documentation that substantiates your answers, such as, copies or examples of policy, examples of metrics, assessments, agreements, architectural or data flow diagrams, reports of compliance, etc.

# 16. Human Resources

### 16-HRS-01 Asset Returns

Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.

### 16-HRS-02 Background Screening

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.

### 16-HRS-03 Employment Agreements

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.

### 16-HRS-04 Employment Termination

Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.

### 16-HRS-05 Portable and Mobile Devices

Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring).

### 16-HRS-06 Non-Disclosure Agreements

Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals.

### 16-HRS-07 Roles and Responsibilities

Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.

### 16-HRS-08 Acceptable Use

Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (*e.g.*, issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (*i.e.*, BYOD) shall be considered and incorporated as appropriate.

### 16-HRS-09 Security Awareness Training

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.

### 16-HRS-10 User Responsibility

All personnel shall be made aware of their roles and responsibilities for:

a) Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.
b) Maintaining a safe and secure working environment

### 16-HRS-11 Workspace

Policies and procedures shall be established to require that unattended workspaces do not have openly visible (*e.g.*, on a desktop) sensitive documents and user computing sessions had been disabled after an established period of inactivity.

### 16-HRS-12A City and County of Denver Data

Policies and procedures shall be established to mandate that data belonging to the City, regardless of encryption state, shall not leave the predefined corporate premise by unauthorized or unapproved means.

## 16. Human Resources

Please provide a short narrative that describes the controls you have in place for the Cloud Security Alliance Cloud Security Matrix control domain listed above. Consult the detailed controls to help clarify the topic. You do not need to directly answer each of the detailed controls; however, your answer must allow us to gain a thorough understanding of your control environment for the domain. You may optionally provide documentation to support your answer in an appendix that you supply. We reserve the right to request documentation that substantiates your answers, such as, copies or examples of policy, examples of metrics, assessments, agreements, architectural or data flow diagrams, reports of compliance, etc.

# 17. Identity and Access Management

### 17-IAM-01 Audit Tool Access

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.

### 17-IAM-02 User Access Policy

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:

a) 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)
b) 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)
c) Access segmentation to sessions and data in multi-tenant architectures by any third party (*e.g.*, provider and/or other customer (tenant))
d) Identity trust verification and service-to-service application (API) and information processing interoperability (*e.g.*, SSO and federation)
e) Account credential lifecycle management from instantiation through revocation

### 17-IAM-03 Diagnostic and Configuration Port Access

User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.

### 17-IAM-04 Policies and Procedures

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.

### 17-IAM-05 Segregation of Duties

User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.

### 17-IAM-06 Source Code Access Restriction

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.

### 17-IAM-07 Third-Party Access

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.

### 17-IAM-08 User Access Restriction and Authorization

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.

### 17-IAM-09 User Access Authorization

Provisioning user access (*e.g.*, employees, contractors, customers (tenants), business partners and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.

### 17-IAM-09A Access Control Rules

The provider shall maintain a detailed description of all roles (*i.e.*, groups, privileges, authorizations, assets and functions) used in the application.

### 17-IAM-10 User Access Reviews

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.

### 17-IAM-11 User Access Revocation

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.

### 17-IAM-12 User ID Credentials

Answered in Section I, 1-CCD-02.

### 17-IAM-13 Utility Program Access

Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.

## 17. Identity and Access Management

Please provide a short narrative that describes the controls you have in place for the Cloud Security Alliance Cloud Security Matrix control domain listed above. Consult the detailed controls to help clarify the topic. You do not need to directly answer each of the detailed controls; however, your answer must allow us to gain a thorough understanding of your control environment for the domain. You may optionally provide documentation to support your answer in an appendix that you supply. We reserve the right to request documentation that substantiates your answers, such as, copies or examples of policy, examples of metrics, assessments, agreements, architectural or data flow diagrams, reports of compliance, etc.

## 18. Infrastructure and Virtualization Security

**18-IVS-01 Audit Logging and Intrusion Detection**

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.

**18-IVS-01B Error Handling**

The provider shall detail how errors occurring during processing will be handled. Some applications should provide best effort results in the event of an error, whereas others should terminate processing immediately.

**18-IVS-02 Change Detection**

The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (*e.g.* dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (*e.g.* portals or alerts).

**18-IVS-03 Clock Synchronization**

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.

**18-IVS-04 Capacity and Resource Planning**

The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.

**18-IVS-05 Vulnerability Management**

Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (*e.g.* virtualization aware).

**18-IVS-06 Network Security**

Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, ports, and compensating controls.

**18-IVS-07 Operating System Hardening and Base Controls**

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.

### 18-IVS-08 Production and Non-Production Environments

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.

### 18-IVS-09 Segmentation

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:

a) Established policies and procedures
b) Isolation of business critical assets and/or sensitive user data and sessions that mandate stronger internal controls and high levels of assurance
c) Compliance with legal, statutory and regulatory compliance obligations

### 18-IVS-10 Migration Data Protection

Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations.

### 18-IVS-11 Hypervisor Hardening

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).

### 18-IVS-12 Wireless Security

Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following:

a) Perimeter firewalls implemented and configured to restrict unauthorized traffic
b) Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (*e.g.*, encryption keys, passwords, and SNMP community strings)
c) User access to wireless network devices restricted to authorized personnel
d) The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network

### 18-IVS-13 Network Architecture

Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.

## 18. Infrastructure and Virtualization Security

Please provide a short narrative that describes the controls you have in place for the Cloud Security Alliance Cloud Security Matrix control domain listed above. Consult the detailed controls to help clarify the topic. You do not need to directly answer each of the detailed controls; however, your answer must allow us to gain a thorough understanding of your control environment for the domain. You may optionally provide documentation to support your answer in an appendix that you supply. We reserve the right to request documentation that substantiates your answers, such as, copies or examples of policy, examples of metrics, assessments, agreements, architectural or data flow diagrams, reports of compliance, etc.

## 19. Interoperability and Portability

**19-IPY-01 APIs**

The provider shall use open and published APIs to ensure the broadest support for interoperability between components and to facilitate migrating applications.

**19-IPY-02 Data Requests**

All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files).

**19-IPY-03 Policy and Legal**

Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage and integrity persistence.

**19-IPY-04 Standardized Network Protocols**

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.

**19-IPY-05 Virtualization**

The provider shall use an industry-recognized virtualization platform and standard virtualization formats (*e,g.*, OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks, available for customer review.

## 19. Interoperability and Portability

Please provide a short narrative that describes the controls you have in place for the Cloud Security Alliance Cloud Security Matrix control domain listed above. Consult the detailed controls to help clarify the topic. You do not need to directly answer each of the detailed controls; however, your answer must allow us to gain a thorough understanding of your control environment for the domain. You may optionally provide documentation to support your answer in an appendix that you supply. We reserve the right to request documentation that substantiates your answers, such as, copies or examples of policy, examples of metrics, assessments, agreements, architectural or data flow diagrams, reports of compliance, etc.

## 20. Mobile Security

### 20-MOS-01 Anti-Malware Awareness Training

Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.

### 20-MOS-02 Application Stores

A documented list of approved application stores has been communicated as acceptable for mobile devices accessing or storing provider managed data.

### 20-MOS-03 Approved Applications

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.

### 20-MOS-04 Approved Software for BYOD

The BYOD policy and supporting awareness training shall clearly state the approved applications and application stores that may be used for BYOD usage.

### 20-MOS-05 Awareness and Training

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.

### 20-MOS-06 Cloud-Based Services

All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.

### 20-MOS-07 Compatibility

The company shall have a documented application validation process to test for device, operating system, and application compatibility issues.

### 20-MOS-08 Device Eligibility

The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.

### 20-MOS-09 Device Inventory

An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices, (*i.e.*, operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD), will be included for each device in the inventory.

### 20-MOS-10 Device Management

A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.

### 20-MOS-11 Encryption

The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technology controls.

### 20-MOS-12 Jailbreaking and Rooting

The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (*e.g.* jailbreaking or rooting) and shall be enforced through detective and preventative controls on the device or through a centralized device management system (*e.g.* mobile device management).

### 20-MOS-13 Legal

The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations over the loss of non-company data in the case that a wipe of the device is required.

### 20-MOS-14 Lockout Screen

BYOD and/or company owned devices shall require an automatic lockout screen, and the requirement shall be enforced through technical controls.

### 20-MOS-15 Operating Systems

Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.

### 20-MOS-16 Passwords

Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.

### 20-MOS-17 Policy

The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).

### 20-MOS-18 Remote Wipe

All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT.

### 20-MOS-19 Security Patches

Mobile devices connecting to corporate networks or storing and accessing company information shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely.

### 20-MOS-20 Users

The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.

## 20. Mobile Security

Please provide a short narrative that describes the controls you have in place for the Cloud Security Alliance Cloud Security Matrix control domain listed above. Consult the detailed controls to help clarify the topic. You do not need to directly answer each of the detailed controls; however, your answer must allow us to gain a thorough understanding of your control environment for the domain. You may optionally provide documentation to support your answer in an appendix that you supply. We reserve the right to request documentation that substantiates your answers, such as, copies or examples of policy, examples of metrics, assessments, agreements, architectural or data flow diagrams, reports of compliance, etc.

## 21. Security Incident and Management, e-Discovery, and Cloud Forensics

### 21-SEF-01 Contact and Authority Maintenance

Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (*e.g.*, change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.

### 21-SEF-02 Incident Management

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.

### 21-SEF-03 Timely Reporting of Security Events

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.

### 21-SEF-04 Incident Response Legal Preparation

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.

### 21-SEF-05 Incident Response Metrics

Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.

## 21. Security Incident and Management, e-Discovery, and Cloud Forensics

Please provide a short narrative that describes the controls you have in place for the Cloud Security Alliance Cloud Security Matrix control domain listed above. Consult the detailed controls to help clarify the topic. You do not need to directly answer each of the detailed controls; however, your answer must allow us to gain a thorough understanding of your control environment for the domain. You may optionally provide documentation to support your answer in an appendix that you supply. We reserve the right to request documentation that substantiates your answers, such as, copies or examples of policy, examples of metrics, assessments, agreements, architectural or data flow diagrams, reports of compliance, etc.

## 22. Supply Chain Management, Transparency, and Accountability

### 22-STA-01 Data Quality and Integrity

Providers shall inspect, account for, and correct data quality errors and risks inherited from partners within their cloud supply-chain. 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.

### 22-STA-02 Incident Reporting

The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (*e.g.* portals).

### 22-STA-03 Network and Infrastructure Services

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.

### 22-STA-04 Provider Internal Assessments

The provider shall perform annual internal assessments of conformance and effectiveness of its policies, procedures, and supporting measures and metrics.

### 22-STA-05 Third Party Agreements

Supply chain agreements (*e.g.*, SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms:

a) 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)
b) 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
c) Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts
d) 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)
e) 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
f) Expiration of the business relationship and treatment of customer (tenant) data impacted

g) Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence

### 22-STA-06 Service Level Governance Reviews

Providers shall review the risk management and governance processes of their partners to ensure that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.

### 22-STA-07 Service Level Metrics

Policies and procedures shall be established, and supporting business processes and technical measures implemented, for maintaining complete, accurate, and relevant agreements (*e.g.*, SLAs) between providers and customers (tenants), with an ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream), and for managing service-level conflicts or inconsistencies resulting from disparate supplier relationships.

### 22-STA-08 Third-Party Assessment

Providers shall assure reasonable information security across their information supply chain by performing a regular review. The review shall include all partners upon which their information supply chain depends.

### 22-STA-09 Third-Party Audit

Third-party service providers shall demonstrate compliance with information security and confidentiality, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at planned intervals to govern and maintain compliance with the service delivery agreements.

## 22. Service Level Management, Transparency, and Accountability

Please provide a short narrative that describes the controls you have in place for the Cloud Security Alliance Cloud Security Matrix control domain listed above. Consult the detailed controls to help clarify the topic. You do not need to directly answer each of the detailed controls; however, your answer must allow us to gain a thorough understanding of your control environment for the domain. You may optionally provide documentation to support your answer in an appendix that you supply. We reserve the right to request documentation that substantiates your answers, such as, copies or examples of policy, examples of metrics, assessments, agreements, architectural or data flow diagrams, reports of compliance, etc.

# 23. Threat and Vulnerability Management

### 23-TVM-01 Anti-Virus and Malicious Software

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.

### 23-TVM-02 Vulnerability and Patch Management

Policies and procedures shall be established, and supporting business processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed (physical and virtual) applications and infrastructure network and system components, applying a risk-based model for prioritizing remediation through change-controlled, vender-supplied patches, configuration changes, or secure software development for the organization's own software. Upon request, provider shall inform customer (tenant) of policies and procedures, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.

### 23-TVM-03 Mobile Code

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.

### 23-TVM-04A Specific Vulnerabilities

The vendor and City shall include a set of specific vulnerabilities that shall not be found in the cloud service. If not otherwise specified, then the cloud service shall not include any of the flaws described in the latest promulgated “OWASP Top Ten Most Critical Web Application Vulnerabilities” and “CWE/SANS TOP 25 Most Dangerous Software Errors.”

## 23. Threat and Vulnerability Management

Please provide a short narrative that describes the controls you have in place for the Cloud Security Alliance Cloud Security Matrix control domain listed above. Consult the detailed controls to help clarify the topic. You do not need to directly answer each of the detailed controls; however, your answer must allow us to gain a thorough understanding of your control environment for the domain. You may optionally provide documentation to support your answer in an appendix that you supply. We reserve the right to request documentation that substantiates your answers, such as, copies or examples of policy, examples of metrics, assessments, agreements, architectural or data flow diagrams, reports of compliance, etc.

### Option 3 – Questionnaire

In some cases, it may be easier for the vendor to answer specific questions instead of creating the narrative to answer the questions. These questions are taken from the Cloud Security Alliance Consensus Assessments Initiative Questionnaire. The information is the same as in Option 2, but in a format that helps guide the vendor through comprehensively answering the questions.

The questionnaire is added as an attachment to this document.