Cybersecurity Risk Assessment

Cybersecurity Risk Assessment

Cyber Risk Categories: The following technology services represent additional cybersecurity risk to the City:

1. **Cloud SaaS Technology:** A software distribution model in which a service provider hosts applications for customers and makes them available to these customers via the internet.

   Examples: Salesforce, Snowflake, Amazon Web Services.
   Exclusions: Software, images or documents to be downloaded, installed and used on City systems.

2. **Operational Technology:** Hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes, and events. OT is common in Industrial Control Systems (ICS) such as a SCADA system.

   Examples: Building Management Systems (BMS), Heater Ventilation Air Conditioning (HVAC)
   Exclusions: OT systems without remote access from the Internet and with no cloud components

3. **Professional Services.** All instances where a non-City employee is given access of any kind to City networks or systems (e.g. IT-support, software installation, etc).

   Examples: Contracting services hired to support applications and data management.
   Exclusions: Training services or services where a contractor does not have access to City data or systems OR they are using City- provided equipment.

4. **Sensitive Data Access:** Contractors that have access to and/or store Level 3-5 City data on their systems during the performance of the contract. Please refer to COIT data classification standard: https://sfcoit.org/datastandard

   Examples: Level 3-5 data includes sensitive and compliance-related data, such as HIPAA, CJIS, and IRS data.
   Exclusions: Level 1-2 public data.

Cybersecurity Risk Assessment Timing: For each technology that qualifies for one or more of the above-named categories, City departments are required to perform Cybersecurity Risk Assessment (CRA) at the following stages of the procurement process:

1. As a solicitation is being conducted, during the evaluation of app responsive proposals or bids being considered; or

2. Where a solicitation is not being conducted, prior to requesting permission from OCA to waive or alter solicitation requirements or in the event of a sole source contract.

Prime Contractors and Resellers: Where the technology and/or technical services are procured through a prime contractor or reseller, CRA must be performed for the entity(ies) responsible for manufacturing the product, performing the technical functions related to the product's performance, and/or accessing City's networks and systems. In some instances where the prime contractor or reseller plays an active role in each of these activities, CRA shall also be required for the prime contractor or reseller.

CRA Reports: To conduct a CRA, the department must collect as part of its solicitation process (or, where there is no solicitation process, upon requesting a quote) one of the following two reports:

1. **SSAE 18 SOC-2 Type 2 Report:** Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy (management's description of a service organization's system and the suitability of the design and operating effectiveness of controls, aka SOC-2 Type 2); or
2. **City Cyber Risk Assessment (CRA) Questionnaire**: City Cybersecurity Risk Assessment questionnaire based on Consensus Assessments Initiative Questionnaire-Lite.

The above reports will be evaluated by the soliciting department and DT to identify existing or potential cyber risks to City which shall be remediated on or before contract execution, but in no event later than 180 days from contract execution (unless otherwise agreed to by City). Such remediation and continuing compliance shall be subject to City's on-going review and audit through industry-standard methodologies, including but not limited to: on-site visits, review of the entities' cybersecurity program, penetration testing, and/or code reviews. For additional guidance regarding this process, please visit Vendor Risk Management.

Departments are required to submit a **Certificate of Completion or affirm that the purchase is out of scope** for the cybersecurity risk assessment as part of the CIO review.