City and County of San Francisco
Office of Cybersecurity

Third-Party Cybersecurity Assessment
Comprehensive User Manual

December 2025

I. Introduction

We would like to take a moment to express our gratitude for the ongoing partnership and collaboration as a third-party provider of goods and services. In accordance with industry standards mandated by the City's cybersecurity policy, all third-party organizations contracted by the City and County of San Francisco (CCSF), providing technology–related goods and services, or having access to the City's data/systems, are required to complete a Cybersecurity Risk Assessment (CRA).

This annual assessment is a critical measure in safeguarding the sensitive information, systems, and services that the City and County of San Francisco (CCSF) rely on. It upholds the integrity of the City's infrastructure and data.

This user manual, designed with your ease of use and convenience in mind, will guide you through common questions and provide information for each scenario you might encounter.

II. Completing your Cybersecurity Risk Assessment (CRA)

The following Third-Party Audit Reports can be used to satisfy CCSF's Cybersecurity Risk Assessment requirement:

- SOC 2 Type 2
- ISO/IEC 27001
- CSA STAR Level 2
- FedRAMP
- StateRAMP
- HITRUSTCSF – *products or services that primarily relate to the Healthcare industry ONLY.*
- PCI DSS Level 1 – *products or services that primarily relate to the Payment Processing industry ONLY.*
- NIST 800-53

In addition to the Third-Party Audit Reports mentioned above, CCSF's CRA requirement can also be satisfied by providing a completed CAIQ Lite Questionnaire, or completing the City's CRA Questionnaire in LogicGate.

III. Frequently Asked Questions

1. We have a portal for self-service security reviews; how can we provide the required information to CCSF?

In the "Third-Party Audit" section, after specifying which third-party audit you would like to provide, select "Third-Party audit can be accessed via trust portal". In the "Trust Portal Link" field, provide your company trust portal link and grant access to City's Technology Risk & Resilience email address: cyber-risk@sfgov.org. Complete all fields and submit the assessment.

Note:

- Organizations that provide professional services and do not have any information on Data Centers can enter "Not Applicable" in the data center fields.

2. An NDA is required before sharing the third-party audit report, how can we proceed?

In the "Third-Party Audit" section, after specifying which third-party audit you would like to provide, select "Attach third-party audit file directly in LogicGate – NDA Required".

By choosing this option, an NDA section will appear, outlining two options:

i. Fastest option – Use CCSF's pre-signed NDA by selecting "Yes, I will use the pre-signed standard NDA template," download the pre-signed NDA, complete the NDA, and upload it along with your specified third-party audit.

ii. Alternative option with delays – Use a proprietary NDA by selecting "No, a proprietary NDA is required", upload your proprietary NDA and submit the assessment. The City's Technology Risk & Resilience team will contact you directly to facilitate completing your proprietary NDA. Once the NDA is completed, your assessment will be sent back to you to upload the third-party audit file into LogicGate.

Note:

- A proprietary NDA must be reviewed by the City and County of San Francisco City Attorney's Office. This option may delay NDA completion.

3. Where is the pre-signed NDA located?

After selecting "Yes, I will use the pre-signed standard NDA template", CCSF's pre-signed NDA template will populate and be available for download and completion.

4. How can we share a third-party audit report when an NDA is not required?

In the "Third-Party Audit" section, after specifying which third-party audit you would like to provide, select "Attach third-party audit file directly in LogicGate – No NDA Required". An attachment field will appear for you to attach your third-party audit file.

5. We cannot provide an accepted third-party audit or CAIQ Lite questionnaire, what is the process to complete the CRA Questionnaire?

In the "Third-Party Audit" section, after specifying that you cannot provide any of the accepting third-party audits and specifying that you cannot provide a completed CAIQ Lite questionnaire, a sample template for CCSF's CRA Questionnaire will appear. Briefly review the questionnaire template document, and answer "Yes" to confirm that you can complete it. The questionnaire will populate directly in LogicGate for you to complete.

Note:

- When "Yes" or "Not Applicable" are selected, you will be prompted with a text area to add an explanation for your answer.
- If a control is being met with the assistance of a third party, please answer "Yes."
- For some control questions, "Not Applicable" will not be an available answer.
- Upload any supporting documents at the end of each control section.
- If you are not able to complete the questionnaire in one sitting, you can close out of the questionnaire and return it at any time using the link in this email. Your answers automatically save.
- If other individuals in your organization need to answer some of the questions, you can forward the email with the link to them, and they can access the questionnaire using the same link. If you forward the email to anyone else, you should ensure that you do not edit the same question simultaneously, which can cause issues when saving the data.

6. **We cannot provide one of the accepted third-party audits, a completed CAIQ Lite questionnaire, and our company cannot complete CCSF's CRA questionnaire. How can we proceed?**

In the "Third-Party Audit" section, after specifying that you cannot provide any of the accepted third-party audits, specifying that you cannot provide a completed CAIQ Lite questionnaire, or CCSF's CRA questionnaire, please state the reason(s) why you or the vendor cannot do so in the required text field and submit the assessment.

Note:

- By pressing the submit button, you confirm that you are not able to provide an accepted third-party audit, completed CAIQ Lite questionnaire, or complete CCSF's CRA Questionnaire. You are considered out of compliance with The City & County of San Francisco's cybersecurity review.

7. **What will happen after the due date lapses?**

The assessment due date is not a hard deadline. However, we recommend aiming to meet the proposed timeline.

8. **What is the next step after submitting the assessment?**

The Office of Cybersecurity - Technology Risk and Resilience Team will review the assessment. If they have any questions or the assessment needs more clarification, they will contact you via a LogicGate update request email notification. The email will include your organization name, assessment current assignee, City and County of San Francisco contact information, the requested updates, and a direct link to the assessment.

IV. Need More Help? – Contact the Technology Risk & Resilience Team

Please contact the Technology Risk & Resilience Team at *cyber-risk@sfgov.org* with any additional questions or clarifications you may have regarding your assessment.

Our team of analysts is happy to help!