Application Approval Process

1) How does the application/service approval process begin?

Three ways the Risk and Compliance team can be brought in to the process:

- The Requestor- The requestor can request an application or cloud service assessment. The sooner the Risk and Compliance team is brought in to the selection and purchasing process, the better. As stated earlier, this process can take anywhere from 4-10 weeks, or longer, depending on the responsiveness of the vendor. Contact the **OIT Help Desk at 303-724-4357 (4-HELP) and open a ticket with the Risk and Compliance team for an "Application Approval".** The Risk and Compliance team will then assess the application you would like to purchase for use with confidential or highly confidential data. The Risk and Compliance team will guide you to an approved product that will suit your needs or if there is no approved application or service that will provide the functionality needed, we will begin the assessment process for the product you would like to use.

    - Choosing an approved third party application or service can save time since they do not have to be reassessed for security.

- Procurement Service Center- If we have not been contacted by the requestor, and Procurement is contacted first, the Procurement Service Center will begin the purchasing process and will contact the Risk and Compliance team if approval is needed due to the fact that the application will hold a particular data type. You can contact the Procurement Service Center by going to https://www.cu.edu/psc/commodity-listing and looking for the specific commodity (in this case: Software), for a contact name.

- Regulatory Compliance- We may also be contacted by Regulatory Compliance as part of the BAA process.

2) The Risk and Compliance team will begin the application assessment process. All applications that will house confidential or highly confidential data will be assessed for appropriate use and according to the type of data, even applications that have already been approved. Any information on vendor contacts that your team can provide, will assist us in getting the right person for initial contact. The sales contact for the vendor normally brings in

additional team members on their end to get us the information we are requesting.

3) Approval or Non-Approval notifications will be sent by the Risk and Compliance team via email, going to the requestors and possibly to Procurement or Regulatory Compliance if we were contacted by their teams. (Note: For those requesting the use of a pre-approved application- Even though an application might be preapproved, there may be conditions. You will notice in the chart that those applications will tell you to contact us.)

4) Procurement and/or Regulatory Compliance teams will continue the process on their end according to the results of the Risk and Compliance team findings.

What types of information do we request from the vendors?

We request the same information from each vendor. The approval process is based on what information the vendor provides, the quality of their security processes and controls, and the data type. We request a third party pen test of their application, an SSAE 16 SOC 2 (Data Center Certification), and answers to a list of questions regarding their organization's security controls.