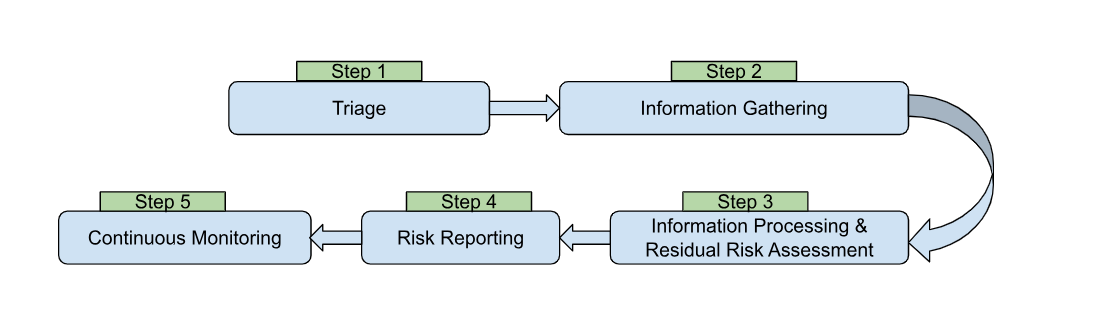
### **Third Party Security Assessment Process Overview**



**Step 1: Triage**

The business requester provides information about the third party engagement to be assessed which the analyst uses to evaluate the inherent risk of the engagement and trigger appropriate security and privacy questionnaire(s). The information provided by the business requester typically includes:

* Details on the third party engagement, such as description of engagement, services being provided, data types being shared, methods of data sharing, and intended use of data.
* Details on the third party such as type and headquarter location.

**Step 2: Information Gathering**

The third party responds to the security and privacy questionnaire(s) triggered during triage and uploads evidence of their organization’s security and privacy posture, if available – such as external certifications/attestations, internal security and privacy policies, and evidence of controls in use at their organization such as antivirus software. The steps taken by the analyst at this point typically include:

* Collecting relevant data about third party’s security and privacy posture through a security questionnaire filled out by the third party.
* Ensuring all documents are current and accurately reflect the third party’s practices and controls.
* Listing all identified risks to assess the effectiveness of third party’s existing controls in mitigating these risks.
* Following up with the third party for confirmation of any additional security and/or privacy controls that are relevant to the engagement use case

**Step 3: Information Processing and Residual Risk Assessment**

The analyst compiles the information gathered to complete the assessment. The steps taken by the analyst include:

* Reviewing the third party’s certifications and policies to evaluate compliance with industry standards.
* Assessing the effectiveness of third party’s existing security and privacy controls.
* Determining the residual risk based on the third party’s inherent risk and effectiveness of the controls.
* Conducting quantitative and qualitative analysis of the potential impact of risks on business operations associated with each third party.

**Step 4: Risk Reporting**

The analyst then documents the third party security and privacy risk for use in enterprise risk quantification and profiling by taking the following steps:

* Preparing a comprehensive report detailing the inherent risk, effectiveness of existing controls, and residual risk of the engagement.
* Identifying gaps in current controls and recommending enhancements to better manage the risks.
* Prioritizing the risks which need more immediate attention or more robust controls.
* Outlining specific actions or mitigation strategies to address risks.

**Step 5: Continuous Monitoring**

The analyst then continuously reviews the third party's security and privacy posture through periodic reassessment or continuous monitoring services by doing the following:

* Conducting regular reassessments of third parties based on the risk exposure and sensitivity of the data involved.
* Ongoing evaluation of the third party's inherent risk and security and privacy posture based on threat feeds, incident reports, etc.
* Developing key performance indicators (KPIs) and metrics to measure the third party’s compliance with security and privacy requirements.
* Reviewing security incidents and remediation plans.