Compliance requirements for Out-sourced Services

Assumption:

- *The requester (service owner is a Cal Poly unit/ employee) is responsible for meeting all applicable policies, standards or regulations.*
- *Must provide all the required documentation*
- *This requirement applies to any third party service provider*

Required documentation for L1 data

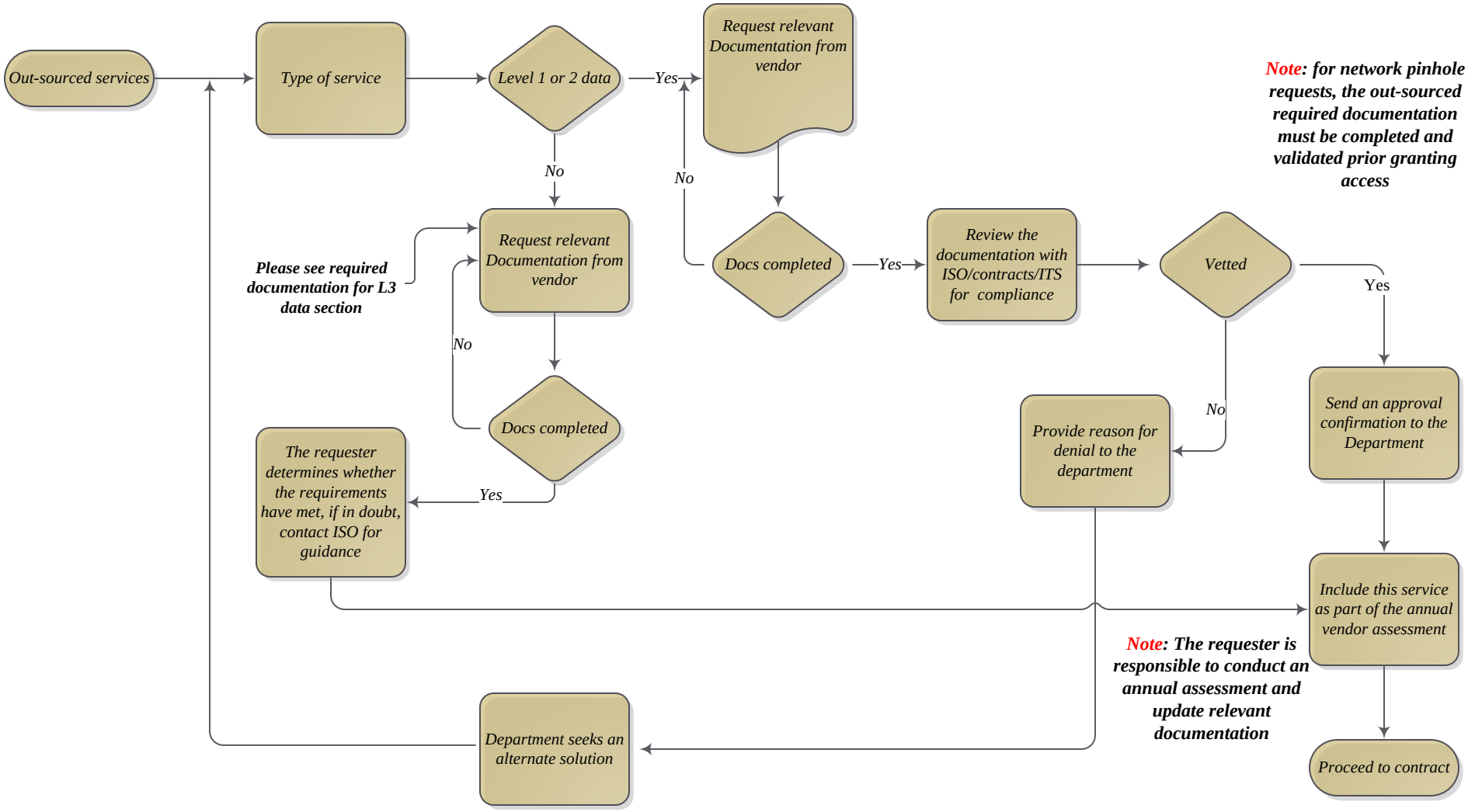
1. Attestation of Compliance (AOC) – (e.g. cert from Cloud Security Alliance or PCI certifications)
2. Industry Standard audit Reports (SOC3, SSAE16, ROC)
3. Contract (ITS Supplemental Provisioning)
4. Dataflow (Card Holder Data Flow)
5. Third-Party Vendor Security Questionnaire
6. Incident Response (this should be included in the contract)
7. Security exception (if needed)
8. Application data request (if needed)
9.. Authentication request (if needed)

Required documentation for L2 data

1. Contract
2. Third-Party Vendor Security Questionnaire
3. Security exception (if needed)
4. Industry Standard audit Reports (SOC3, SSAE16, ROC)
5. Application data request (if needed)
6. Authentication request (if needed)

Required documentation for L3 data

1. Contract
2. Third-Party Vendor Security Questionnaire
3. Security exception (if needed)



***Note**: for network pinhole requests, the out-sourced required documentation must be completed and validated prior granting access*

***Note**: The requester is responsible to conduct an annual assessment and update relevant documentation*