Cloud Vendor Exception Workflow

Vendor completes Vendor Readiness Assessment Report (VRAR)

Agency reviews VRAR for State compliance

Agency approves VRAR and completes Privacy Threshold Analysis (PTA)

Vendor completes Vendor Readiness Assessment Report (VRAR)

Public or Restricted/Highly Restricted Data?

Public Data

Existing Contract/Service?

New or Existing Service?

New Contract/Service?

3rd Party Attestation?

Yes

Done

Vendor Provide 3rd Party Attestation Report

Vendor completes CSET, and provides Vuln/Pen Scan Report (scan must be within 30 days), Vuln Mgmt Plan, IR Plan, BC Plan, and Security Policy

Vendor MUST formally agree to complete a 3rd Party Attestation within 1 year! (Agency contract must enforce financial penalties for non-compliance)

Vendor provide 3rd Party Attestation and annual updates to Agency

Reject Vendor

Third Party Attestation Report includes SOC 2 Type 2, FedRAMP, and ISO 27001. Note: An IaaS vendor (e.g. AWS) cannot provide a certification for a SaaS provider UNLESS that is written in the agreement between the 3rd and 4th party vendor.