Third-Party Security Assessment Process

OMES Cyber Command supports an extensive third-party risk management program to meet the needs of the state's diverse supply chain. By vetting not only our primary supplier's security posture but also their subcontractors and other downstream providers, we ensure that the state's data and systems remain protected.

For a company to access, process, store or transmit state data, they must have an Authority to Operate Order (AOO) signed by the state Chief Information Security Officer (CISO) or designee. An AOO is produced after a thorough security assessment has been reviewed by OMES Cyber Command.

Questions? Email us at thirdpartysecurity@omes.ok.gov.

Third-Party Security Assessment Process

Use this process to establish an Authority to Operate order for a new supplier.

Step 1:

Security analyst sends supplier a security assessment. Supplier completes.

Step 2:

Analyst reviews responses. If there are any questions or issues, the analyst works with the supplier to resolve.

Step 3:

Once the assessment is complete, a security engineer reviews the document.

If approved, engineer submits approval to analyst for crafting of AOO.

If not approved, the analyst and supplier work to resolve issues.

Step 4:

CISO signs AOO and analyst issues to supplier.

Third-Party Security Assessment Process

Use this process to renew an Authority to Operate order that is older than one year.

Step 1:

For suppliers whose AOO has expired, a security analyst requests an updated security assessment or an attestation on company letterhead indicating the supplier's security posture has not deteriorated since the execution date on their last AOO.

Step 2:

For a new, full assessment, the same steps as above are completed.

Step 3:

For an attestation, the supplier completes the document and submits for approval.

Step 4:

CISO signs renewed AOO and analyst issues to supplier.