Third-Party Risk Management Standard

Introduction

OMES Information Services is committed to preventing incidents that may impact the confidentiality, integrity or availability of information assets through third-party risk management for the State of Oklahoma. Third-party risk management is a critical component of the OMES IS information security program, which helps ensure any risk to confidentiality, integrity or availability is identified, analyzed and maintained at acceptable levels.

State policy requires the performance of routine assessments to identify risk and ensure appropriate controls. Security assessments allow the alignment of information security with business objectives and regulatory requirements. Identifying information security risk and control requirements from the onset is essential and far less costly than retrofitting or addressing the impact of a security incident. Furthermore, these assessments allow management to prioritize and focus on areas that pose most significant impact on critical and sensitive information assets, providing the foundation for informed decision-making regarding information security.

OMES IS considers vulnerabilities, threat sources and planned or currently placed security controls. These inputs help determine the resulting level of risk posed to information, systems, processes and individuals that support business functions. While third-party risk management and related assessments take many forms (e.g., audits, security reviews, configuration analysis, vulnerability scanning and testing), they all have the same goal: to improve overall security posture by identifying and acting on risk. An entity can never truly eliminate risk but can take steps to manage it.

As per OMES IS policy, any supplier accessing, processing, storing or transmitting State of Oklahoma data must be appropriately managed for risk and undergo risk assessments as part of its life cycle.

Purpose

This document establishes the requirement for third-party assessments for suppliers accessing, processing, transmitting or storing data in compliance with OMES IS security policies, standards and procedures.

Definitions

Third-party – Any contractor, service provider, consultant or any other individual and/or organization external to state government providing services on behalf of, for, or as an agent of state government.

Low risk – Any system or data intended for public disclosure. The loss of confidentiality, integrity or availability of the system or data would have no adverse impact on safety, finances or reputation.

Moderate risk – Any system or data not generally available to the public. The loss of confidentiality, integrity or availability of the system or data could have a mildly adverse impact on safety, finances or reputation.

High risk – Any system or data protected by law or regulation (e.g., FTI, CJI, PHI, PII and PCI). The loss of confidentiality, integrity or availability of the data or system could significantly and adversely impact safety, finances or reputation. The type of risk requires the state to self-report to the regulatory entity and/or notify the individual if data is inappropriately accessed.

Standard

The state agency shall categorize data as confidential by system owners, including protected health information and personally identifiable information, in accordance with applicable federal and state laws, directives, standards, guidance, policies and regulations.

OMES IS shall conduct third-party security assessments. The assessment should address the likelihood and magnitude of harm should there be unauthorized access, use, disclosure, disruption, modification or destruction of the information system and the information it processes, stores or transmits. Additionally, these guidelines apply to risk assessments:

- OMES IS shall document risk assessment results in an annual risk assessment.
- OMES IS shall review risk assessment results annually.
- OMES IS shall disseminate risk assessment results to stakeholders.
- OMES IS shall update the third-party security assessment annually or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities) or other conditions that may impact the system's security state.

All third parties given access to State of Oklahoma information, information systems or information assets must complete a security assessment. The purpose of the assessment is for the State of Oklahoma to identify and manage the risk stemming from the business partnership.

A supplier is required to complete an assessment if accessing, processing, storing or transmitting State of Oklahoma data. The assessment is not restricted to a specific service or solution but is for the vendor to be assessed from an internal security standpoint. The security of the tools, platforms or procedures used should have no bearing on the enterprise security controls of the supplier.

Industry-standard assessments and certifications may be used in lieu of the OMES IS assessment if they are substantially similar in structure and content. The following industry-standard assessments and certifications are approved.

- SIG Lite for low-risk suppliers.
- SIG Core for moderate- to high-risk suppliers.
- CSA CAIQ v3.1 for low- to high-risk cloud providers.
- CSA CCM/CAIQ v4 for low- to high-risk cloud providers.
- FedRAMP for low- to high-risk cloud providers.
- StateRAMP for low- to high-risk providers.

Compliance

This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination.

Rationale

To coordinate and require central approval of state agency information technology purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure that the state delivers

essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

References

- National Institute of Standards and Technology Special Publications: NIST SP 800-53a –Risk Assessment, NIST SP 800-12, NIST SP 800-30, NIST SP 800-39, NIST SP 800-40, NISTSP 800-70, NIST SP 800-100 and NIST SP 800-115; NIST Federal Information Processing Standards 199.
- Attachment D State of Oklahoma IT Terms.
- State of Oklahoma Information Security Policy, Procedures, Guidelines.
- Cloud Security Alliance (CSA).
- Shared Assessments (SIG).
- FedRAMP Authorization Management Program.
- StateRAMP.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 11/06/2020	**Review cycle:** Quarterly
Last revised: 11/18/2021	**Last reviewed:** 11/17/2022
Approved by: Jerry Moore, Chief Information Officer	