OMES Information Technology Risk Management Policy

Introduction

This Risk Management Policy establishes a structured and integrated approach to managing risk in alignment with the principles and guidelines of ISO 31000. The purpose of this policy is to establish a consistent framework for identifying, assessing, mitigating, monitoring, and communicating information technology risks throughout the State. This policy supports the protection of Agency information assets, ensures compliance with applicable Oklahoma statutes and OMES Chief Information Officer ("CIO") Standards, and promotes informed risk-based decision making throughout the technology lifecycle. The OMES CIO Standards establish enterprise technology requirements designed to reduce risk through consistent governance, security practices, architectural alignment, protection of information resources, and responsible management of technology services.

Purpose

This policy applies to State agencies as defined by 62 O.S. § 35.3 (6) including OMES, third parties with access to agency information systems or data, information assets, applications, cloud services, artificial intelligence solutions, infrastructure, software, hardware, and technology services owned, operated, managed, or used by State agencies. It applies to all types of risk, including strategic, operational, financial, legal, regulatory, technological, cybersecurity, reputational, and environmental risks. Risk management shall be applied consistently across the organization and integrated into all significant activities and decision-making processes.

Policy

I. Risk Management Principles

In accordance with ISO 31000, the risk management framework shall be based on the following principles:

Risk-Based Decision Making. Technology decisions shall consider the potential impact to State agency operations, State information resources, security obligations, and business objectives. The State agency should evaluate technology risks before implementing new technology solutions or making significant changes to existing technology environments.

Standardization Reduces Risk. State agencies shall utilize established technology standards to reduce risks associated with inconsistent configurations, unsupported technologies, security weaknesses, interoperability issues, and inefficient technology investments. The OMES CIO Standards provide a consistent framework for technology governance, architecture, security, and operational management.

Security and Privacy by Design. Security considerations shall be incorporated into technology planning, acquisition, implementation, and operation. Technology solutions shall be evaluated to ensure appropriate protections are implemented to safeguard State information resources.
Least Privilege and Controlled Access. Access to State agency technology resources shall be managed to reduce the risk of unauthorized access, misuse, or exposure of information resources. Access should be based on authorized business requirements and managed throughout the user and system lifecycle.

Continuous Monitoring and Improvement. Technology risks change over time due to evolving threats, vulnerabilities, business requirements, and technology changes. The State shall continuously evaluate technology risks and adjust controls as necessary to maintain an effective risk management program.

To implement these principles, State shall:

1. Identify technology risks before implementing new technology or significant changes.
2. Evaluate risks based on the potential impact to State agency operations, information assets, and State services.
3. Implement appropriate administrative, technical, and operational safeguards to reduce identified risks.
4. Continuously monitor risks throughout the lifecycle of technology solutions.
5. Document significant risks and risk treatment decisions.
6. Escalate risks that exceed the State agency's acceptable risk tolerance to appropriate leadership.
7. Review risk whenever material changes occur to systems, services, suppliers, or business operations.

II. OMES CIO Standards

State agencies shall use the OMES CIO Standards as the foundation for managing technology risks. The CIO and OMES IS manages statewide information technology risk through the establishment, governance, and implementation of CIO Standards. The CIO Standards provide a consistent framework for identifying, evaluating, mitigating, and monitoring technology risks across the State enterprise. These standards establish governance, security, architecture, and operational requirements designed to reduce risk and support the secure, reliable, and effective use of information technology resources.

A. Enterprise Governance Risk

To reduce the risk associated with inconsistent technology decision-making, OMES establishes governance practices consistent with applicable CIO Standards, including the Enterprise Governance Standard, Reference Architecture Standard, and Software Architecture Standard. These standards establish a framework for evaluating technology solutions, promoting enterprise alignment, and ensuring technology investments support business objectives while reducing unnecessary complexity.

OMES considers enterprise architecture, technology alignment, integration requirements, security considerations, and long-term operational impacts when evaluating technology solutions. By requiring governance and architectural consideration before implementing technology solutions, OMES reduces the risk of technology duplication, unsupported solutions, increased maintenance complexity, security weaknesses caused by inconsistent implementation, and investments that do not align with enterprise technology objectives.

B. Technology Acquisition Risk

To reduce technology acquisition risk, OMES establishes requirements for evaluating technology purchases, subscriptions, services, and solutions in accordance with applicable laws, procurement rules, and CIO Standards before implementation. Applicable standards include, but are not limited to, the Supply Chain Security Standard, Software Licensing Standard, Software Architecture Standard, Reference Architecture Standard, Security Standards, Accessibility Standards, and Use of AI in Oklahoma State Government Standard. OMES evaluates technology solutions to ensure they meet applicable security, architectural, operational, and compliance requirements throughout the acquisition lifecycle. By incorporating

risk evaluation into technology acquisition processes, OMES reduces the risk of procuring unsupported or insecure technologies, introducing unauthorized solutions into the environment, creating unexpected operational dependencies, acquiring technology that cannot meet security requirements, and incurring avoidable costs associated with replacement or remediation.

C. Supply Chain and Third-Party Risk

To reduce supply chain risk, OMES implements controls consistent with the OMES Supply Chain Security Standard and Contractor Requirements Standard. OMES evaluates suppliers and third-party technology providers to understand risks associated with third-party access, software and technology components, service dependencies, security practices, data handling practices, and operational reliance on external providers.

Supplier risk management is incorporated throughout the technology lifecycle, including procurement, implementation, operation, and termination. By applying supply chain security practices, OMES reduces the risk of compromised software or technology components, unauthorized access by third parties, loss of control over State information, operational disruptions caused by supplier failures, and security vulnerabilities introduced through external dependencies.

D. Artificial Intelligence Risk

To reduce risks associated with artificial intelligence, OMES establishes artificial intelligence governance practices consistent with the OMES Use of AI in Oklahoma State Government Standard. AI solutions are evaluated before use to ensure appropriate consideration is given to the intended use, data involved, security considerations, risks associated with outputs, appropriate human oversight, and compliance with applicable requirements.

AI solutions are managed throughout their lifecycle to ensure continued alignment with approved use cases and applicable security expectations. By applying AI governance requirements, OMES reduces the risk of unauthorized use of AI technologies, exposure of sensitive or protected information, reliance on inaccurate or inappropriate AI-generated content, lack of accountability for AI-supported decisions, and deployment of AI solutions without appropriate review.

E. Data Security and Information Protection Risk

To reduce information security risks, OMES establishes protections consistent with the OMES Data Security Standard and applicable security standards. State information shall be appropriately protected throughout its lifecycle, including collection, storage, processing, transmission, sharing, and disposal.

OMES considers information sensitivity, access requirements, security protections, and applicable handling requirements when establishing data protection requirements. By implementing data security controls, OMES reduces the risk of unauthorized disclosure of State information, loss or corruption of information, improper access to protected data, inadequate protection of information assets, and failure to meet security obligations.

F. Identity and Access Management Risk

To reduce identity and access risks, OMES establishes identity management requirements consistent with the OMES Identity Management Standard. Access to State systems shall be managed throughout the identity lifecycle, including account creation, modification, and removal. OMES establishes requirements to ensure access is appropriately controlled based upon authorized business requirements. By implementing identity management controls, OMES reduces the risk of unauthorized system access, excessive privileges, orphaned accounts, improper access to State information, and unauthorized changes to technology resources.

G. Application Security Risk

To reduce application security risks, OMES establishes application security requirements consistent with the OMES Application Security Standard. Application security shall be considered throughout the application lifecycle, including design, development, acquisition, implementation, maintenance, and retirement.

By incorporating security practices throughout the application lifecycle, OMES reduces the risk of exploitable application vulnerabilities, unauthorized access through applications, data exposure caused by insecure applications, and operational disruptions caused by application weaknesses.

H. Software Licensing Risk

To reduce software licensing risks, OMES establishes software management requirements consistent with the OMES Software Licensing Standard. Software shall be appropriately managed to ensure authorized use, appropriate licensing, and effective lifecycle management. By maintaining software licensing controls, OMES reduces the risk of unauthorized software use, licensing violations, unexpected costs, unsupported software deployments, and increased security exposure from unmanaged software.

I. Vulnerability Management Risk

To reduce cybersecurity risks associated with vulnerabilities affecting State technology resources, OMES establishes vulnerability management requirements consistent with the OMES Vulnerability Management Standard. The Agency shall maintain processes to identify, evaluate, prioritize, and remediate vulnerabilities affecting information technology resources based upon risk, severity, and potential impact to State operations. Vulnerability management activities shall support the identification of vulnerabilities, evaluation of associated risks, prioritization of remediation activities, tracking of mitigation efforts, and validation that appropriate remediation has occurred.

By implementing vulnerability management practices, OMES reduces the risk of exploitation of known vulnerabilities, unauthorized access to systems, malware infections, service interruptions, compromise of State information resources, and increased cybersecurity exposure.

J. Security Management Risk

To reduce information security risks associated with inadequate protection of State technology resources, OMES establishes security requirements consistent with applicable OMES security-related CIO Standards, including standards addressing information security, data security, application security, identity management, vulnerability management, acceptable use, supply chain security, and security operations. Security requirements shall be incorporated throughout the technology lifecycle and applied to State systems, applications, infrastructure, and services. OMES shall utilize a risk-based approach to identify security requirements and establish appropriate protections based on the sensitivity of information resources, operational requirements, and potential impacts.

By implementing security standards and practices, OMES reduces the risk of unauthorized access, security incidents, data compromise, system disruption, improper use of technology resources, and failure to protect State information resources.

K. Network and Infrastructure Risk

To reduce risks associated with network and infrastructure operations, OMES establishes requirements consistent with applicable Network and Server Standards and Enterprise Systems Standards. Network and infrastructure components shall be managed using consistent practices

for configuration, maintenance, security, availability, performance, lifecycle management, and operational support. OMES shall establish requirements designed to ensure infrastructure components are maintained in supported configurations and managed in a manner that supports secure, reliable, and effective technology operations.

By implementing standardized network and infrastructure practices, OMES reduces the risk of unsupported technology, misconfigured systems, security weaknesses, service interruptions, increased maintenance complexity, and failure of critical technology services.

L. Workplace Technology Risk

To reduce risks associated with workplace technology resources, OMES establishes requirements consistent with applicable Workplace Services Standards. Agency-managed workplace technologies shall be maintained in accordance with established requirements for device management, configuration, security protections, software management, and user access. OMES establishes requirements to support consistent management and protection of workplace technology resources throughout their lifecycle.

By implementing workplace technology controls, OMES reduces the risk of compromised user devices, unauthorized access, loss of State information, introduction of malicious software, and inconsistent security configurations.

M. Business Continuity and Disaster Recovery Risk

To reduce operational resilience risks associated with technology disruptions, cybersecurity incidents, disasters, equipment failures, and other events that may impact State services, OMES establishes requirements consistent with the Business Continuity and Disaster Recovery Standard. OMES establishes requirements for identifying critical technology services and supporting appropriate recovery capabilities based on business requirements. Business continuity and disaster recovery practices shall address the recovery of technology resources, restoration of information resources, operational impacts of disruptions, and ongoing improvement of recovery capabilities.

By implementing continuity and disaster recovery practices, OMES reduces the risk of extended service outages, loss of critical business functions, inability to recover from disruptive events, permanent loss of information, and operational impacts caused by technology failures.

N. Offshore Data Storage Risk

To reduce risks associated with offshore storage or processing of State information, OMES establishes requirements consistent with the Offshore Data Storage Standard. OMES evaluates where State information is stored, processed, and accessed to ensure appropriate protections, oversight, and risk management practices are maintained. OMES considers jurisdictional requirements, security protections, access considerations, and operational impacts associated with offshore storage or processing of State information.

By managing offshore data storage risks, OMES reduces the risk of loss of control over State information, unanticipated legal or regulatory obligations, inadequate security protections, unauthorized access, and challenges associated with incident response or recovery.

O. Acceptable Use Risk

To reduce risks associated with inappropriate use of State technology resources, OMES establishes requirements consistent with the Acceptable Use Standard. State technology resources shall be used appropriately, responsibly, and only for authorized purposes. OMES establishes expectations regarding the appropriate use of technology resources and workforce responsibilities when accessing State systems and information.

By implementing acceptable use requirements, OMES reduces the risk of unauthorized activities, security incidents caused by user actions, improper disclosure of information, misuse of State resources, and introduction of security threats.

P. Permitted and Prohibited Technology Risk

To reduce risks associated with unauthorized, unsupported, or insecure technologies, OMES establishes requirements consistent with the Permitted Technology Standard and Prohibited Technology Standard. Technology solutions shall be evaluated to determine whether they align with approved technology requirements and whether they introduce unacceptable security, operational, or compliance risks. Technologies that create unacceptable risk shall not be implemented or utilized within the State technology environment.

By maintaining approved technology requirements, OMES reduces the risk of unsupported technology deployments, security vulnerabilities, inconsistent technology environments, increased operational complexity, and exposure caused by prohibited technologies.

Q. Information and Communication Technology Accessibility Risk

To reduce accessibility risks associated with technology solutions that may prevent individuals with disabilities from accessing State information and services, OMES establishes requirements consistent with the Accessibility of Information and Communication Technology Standard Accessibility requirements shall be considered throughout technology planning, procurement, development, implementation, and operation.

By implementing accessibility requirements, OMES reduces the risk of barriers to accessing State services, noncompliant technology solutions, inequitable access to information resources, and remediation costs associated with inaccessible technology.

R. Contractor and External Personnel Risk

To reduce risks associated with contractor and external personnel access to State systems, information, and facilities, OMES establishes requirements consistent with the Contractor Requirements Standard. Contractors and external personnel shall comply with applicable technology, security, and information protection requirements when performing services for the State.

By managing contractor and external personnel access, OMES reduces the risk of unauthorized access, improper handling of State information, security incidents involving third parties, failure to meet security obligations, and loss of accountability for external users.

III. Leadership and Governance

Leadership and commitment are essential to the effectiveness of risk management. OMES will maintain a Risk Management Team (RMT) to provide enterprise-level oversight and direction. The RMC will meet at least quarterly to review the organization's risk profile, assess significant and emerging risks, evaluate the effectiveness of controls, and ensure alignment with the organization's risk appetite and strategic objectives.

Each OMES IS Pillar lead is accountable for implementing and maintaining risk management processes within their pillar. Pillar leads will ensure that risks are identified, analyzed, evaluated, treated, monitored, and reported in accordance with this policy. They will review and validate risk entries submitted by employees, oversee mitigation progress, and ensure that quarterly updates are completed. Pillar leads will escalate significant risks to the RMT as appropriate.

IV. Risk Assessment and Evaluation

OMES shall apply a consistent, risk-based methodology to identify, analyze, evaluate, and monitor information technology risks. Risk assessments shall support informed decision-making and ensure technology risks are managed in a manner consistent with the State agency's mission, strategic objectives, and risk tolerance. When identifying and assessing risks, OMES shall establish the context by considering applicable internal and external factors that may influence the likelihood or impact of a risk. These factors include, but are not limited to, the State agency's strategic objectives, statutory and regulatory requirements, business and operational environment, technology environment, stakeholder expectations, organizational capabilities, and dependencies on third-party providers or other external entities.

OMES shall identify technology risks that may affect the confidentiality, integrity, availability, security, or reliability of State information resources or otherwise impede the achievement of State agency objectives. Identified risks shall be documented. Each identified risk shall be analyzed to determine its likelihood of occurrence and potential impact using the risk assessment methodology. Risk analysis shall consider the effectiveness of existing controls and evaluate both the inherent risk, representing the level of risk before the application of controls, and the residual risk remaining after existing controls and mitigation measures have been considered.

Following analysis, OMES shall evaluate identified risks against the risk appetite and risk tolerance to determine whether additional mitigation, acceptance, transfer, avoidance, or escalation is warranted. Risks that exceed established thresholds shall be prioritized for treatment, assigned to an appropriate risk owner, and escalated to leadership when necessary to support timely risk-informed decision-making. Risk assessments shall be reviewed and updated whenever significant changes occur to technology, business operations, suppliers, regulatory requirements, threat conditions, or other factors that may materially affect the risk posture.

V. Risk Monitoring and Continuous Improvement

OMES is committed to continual improvement of its risk management framework and processes. Risk monitoring activities shall consider changes to technology environments; changes to business requirements; new vulnerabilities or threats; changes to applicable CIO Standards; security incidents, audit findings; and operational performance. Lessons learned from risk events, audits, monitoring activities, and RMT reviews will be used to strengthen risk management practices. This policy will be reviewed annually by the RMT to ensure alignment with ISO 31000 principles, changes to CIO Standards, changes in technology risk, applicable legal or regulatory requirements and evolving organizational needs.

Compliance

This policy shall take effect upon publication. OMES divisions may amend and publish the amended policies at any time. OMES employees are expected to comply with all published policies and any published amendments thereof and, if found in violation of this policy, may be subject to disciplinary action, up to and including termination. This policy is recommended as a guideline for other state employees.

Revision history

This policy is subject to periodic review to ensure relevancy.

Effective date: 07/14/2026	**Review cycle:** Annual
Last revised: 07/14/2026	**Last reviewed:** 07/14/2026
Approved by: Dan Cronin, Chief Information Officer	