COLORADO
Governor's Office of Information Technology

Office of the Governor

Governor's Office of Information Technology
Information Technology Lifecycle Planning
8 CCR 1501-12

Summary

This is a high-level summary of how the rules work, not part of the rules themselves.

1) Non-consolidated agencies provide OIT with information about IT assets that receive an appropriation through the IT capital asset request process.
2) Consolidated agencies assist OIT in building a comprehensive inventory of IT assets.
    a) For the purposes of these rules, IT assets are defined not by their financial cost, but by their information security risk and connection to state networks. IT assets identified by these rules may differ from IT assets identified according to financial standards.
    b) OIT will develop a phased approach for populating the initial inventory.
    c) The inventory list gets updated more frequently for aging and unsecure IT assets outside the risk boundaries.
3) OIT will provide reports to JBC and JTC regarding aging and unsecure IT assets at consolidated agencies. OIT will provide reports to OSPB regarding the IT assets from consolidated agencies and non-consolidated agencies making ADLE payments, and the amount of money needed to make ADLE payments.
4) OIT will note agencies' failure to comply with the rules (i.e., contribute their IT inventory data points) in its reports to JBC, JTC and OSPB.

5) Define the boundaries of unacceptable risks for aging and unsecure IT assets at consolidated agencies.
6) For consolidated agencies, OIT will work with agencies to prioritize attention and possible limiting actions to mitigate the risks from IT assets outside the risk boundaries.
7) Consolidated agencies may request exceptions and appeal OIT lifecycle plan actions.

12.1 Authority

The Chief Information Officer in the Office of Information Technology (OIT) is authorized and directed by the provisions of section 24-37.5-106 (4), C.R.S. and section 24-37.5-126, C.R.S. to promulgate rules to establish a technology lifecycle plan. The rules enable the development and delivery of the annual fiscal impact analysis, as directed in section 24-37.5-127 (3), C.R.S., and the annual estimate of the state's technical debt environment, as directed in section 24-37.5-805, C.R.S.

The rules are intended to be consistent with the requirements of the State Administrative Procedure Act, section 24-4-101 et seq., C.R.S. (the "APA").

12.2 Scope and Purpose

A. The primary goal is to ensure that technology supports the mission of providing government services. Information technology must be reliable, predictable, and perform adequately to fulfill its intended purpose.
B. These rules ensure that the State of Colorado's information technology assets and systems are inventoried, categorized, and managed. This allows the State to make well-informed decisions and develop effective strategies for growth, scalability, cost optimization, privacy, security, consistent workflows, stability, reliability, and customer experience.
C. The rules address various factors that impact the lifecycle cost of technology, including information security risks, infrastructure risks, operating cost misalignment, productivity cost misalignment, and talent depreciation.

D. These rules enable the State to plan for the orderly and predictable funding, acquisition, deployment, operation, maintenance, and decommissioning of IT assets.

12.3 Applicability

A. The rules apply to all IT assets used by state agencies as defined in section 24-37.5-102(28), C.R.S., including all IT capital projects that receive funding from the capital construction section of the annual general appropriation act. These IT assets encompass IT infrastructure, information systems, applications, databases, cloud services, and other IT equipment.
B. The rules apply to state agencies as defined in section 24-37.5-127(1)(h), C.R.S. for all information technology capital projects that receive an appropriation in the capital construction section of the annual general appropriation act, beginning with the fiscal year 2025-26 annual general appropriation act.

12.4 Definitions

Cloud service: A cloud service is any type of computing resource or service that is delivered over the internet rather than being hosted or managed on-premises. These services can include:

A. Infrastructure as a Service (IaaS): Providing fundamental computing resources like servers, storage, and networking.
B. Platform as a Service (PaaS): Offering a cloud-based platform for developing, running, and managing applications using programming languages and tools supported by the provider.
C. Software as a Service (SaaS): Delivering ready-to-use software applications over the internet, typically accessed through a web browser or mobile app, without local installation or maintenance.

Consolidated agency: This term refers to executive branch agencies whose IT functions were consolidated under OIT on July 1, 2008, pursuant to SB 08-155 and defined in C.R.S. 24-37.5-102(28).

Information technology annual depreciation-lease equivalent (ADLE) payment: Has the same meaning as defined in C.R.S. 24-37.5-127(1)(f), which means an amount equivalent to the recorded depreciation or amortization of the information technology asset acquired, repaired, improved, replaced, renovated, or constructed with an appropriation from the information technology capital account in the capital construction fund based on the depreciation period, as calculated by the state agency or the state institution of higher education, which calculation a state institution of higher education shall report to the Department of Higher Education. The amount is calculated from the date of acquisition or completion of the repair, improvement, replacement, renovation, or construction to June 30 of the fiscal year of acquisition or completion. The amount continues to be annually calculated on a fiscal year basis until the depreciation for the information technology asset is no longer recorded.

IT asset: Any software, hardware, or virtual machine that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information within an information technology environment and that:

A. Connects to a state agency network either directly or indirectly via a link to other IT assets that are connected to a state agency network; or
B. Needs operational support, which may come from a state agency, OIT, a vendor, or another source.

   IT assets include but are not limited to:

   1. Physical resources like servers, routers, and switches;
   2. Logical resources like software, middleware, operating systems, applications, data files, cloud services, consolidated data center services;
   3. IT communications resources like local area networks (LANs) and wide area networks (WANs) and their components;
   4. Devices connected to a state agency's network include network-connected TVs, HVAC equipment, electric vehicles, cameras, and drones.

IT assets do not include:

1. Consumables and peripheral devices like keyboards, projectors, speakers, scanners, monitors, and mice;
2. Cell phones and mobile devices;
3. Printers;
4. Devices that do not connect to a state agency network;
5. Personal devices that are not owned or supported by OIT or a state agency.

Non-consolidated agency: Refers to any state agency that is not among those executive branch agencies whose IT functions were consolidated under OIT on July 1, 2008, pursuant to SB 08-155 and defined in C.R.S. 24-37.5-102(28).

Operating system: Information system software that manages computer hardware and software resources and provides common services for computer programs. System software supports and manages a computer's basic functions, such as scheduling tasks, executing applications and controlling peripherals (e.g., monitor, mouse, keyboard, speakers).

Operational support: Refers to ongoing activities and resources required to keep an IT asset functioning effectively and securely throughout its lifecycle within the IT environment. This includes a wide range of functions, such as: maintenance, troubleshooting, monitoring performance, managing configurations, security, providing assistance to users who interact with the IT asset, and end-of-life management.

State agency: Has the same meaning as defined in C.R.S. 24-37.5-127(1)(h), which means any department, commission, council, board, bureau, committee, institution of higher education, agency, or other governmental unit of the executive, legislative, or judicial branch of state government that receives an appropriation or is otherwise included in the annual general appropriation act or the annual legislative appropriation act.

Technical debt: Cost of work needed to bring information technology into a state of general good repair (including replacing code, addressing security risks, moving off of

outdated hardware, etc.). Generally, technical debt is characterized by one or more of the following risks or costs:

A. Information security risk, in which the continued operation of the technology is not compliant with modern, generally acceptable standards (e.g., continuing to operate technology after the vendor's publicly documented end-of-life notification).
B. Infrastructure risk, in which the technology stack is unsustainable based on hardware (e.g., replacement parts are no longer available), software (e.g., developers with the required skill set are no longer available), or foundation (e.g., the data center housing the technology is susceptible to social unrest, weather, etc.).
C. Operating cost, in which running costs no longer align with typical benchmarks for a given piece of software. Note that the opposite – no charge – may also be an indicator of technical debt in that the vendor is no longer charging for the use of the technology and an organization may fall into the trap of continuing to operate deprecated technology past its maintained life.
D. Productivity cost, in which the technology users are unable to produce operational output on par with generally accepted standards (e.g., payroll cost per employee is twice the national standard).
E. Talent depreciation, in which employees sustaining outdated technology lose or no longer have skill sets to remain competitive on the open market.

TIOBE index: The TIOBE programming community index is a measure of popularity of programming languages, created and maintained by the TIOBE Company based in Eindhoven, the Netherlands. The index is calculated from the number of search engine results for queries containing the name of the language. The index covers searches in 25 popular search engines. TIOBE focuses on Turing complete languages, so it does not provide information about the popularity of, for instance, HTML. The TIOBE index is not about the best programming language or the language in which most lines of code have been written, but rather may reflect the number of skilled engineers, courses and jobs worldwide. The TIOBE index is available at no cost in an electronic form online at https://www.tiobe.com/tiobe-index/

12.5 Inventory of IT Assets

A. OIT shall develop, document, and maintain an inventory of state agency IT assets that receive an appropriation in the capital construction section of the annual appropriation act, beginning with the fiscal year 2025-26 annual general appropriation act. OIT uses this inventory to complete legislatively mandated reports that provide a statewide perspective of information technology used by state agencies.
    1. Non-consolidated agencies shall contribute data points required by OIT in the format and according to the timing designated by OIT.
    2. For the purposes of these rules, non-consolidated agencies shall only report about information technology capital projects subject to ADLE payments.
    3. Institutions of higher education shall report to the Department of Higher Education. The Department of Higher Education shall report to OIT. For the purposes of these rules, institutions of higher education shall only report about information technology capital projects subject to ADLE payments.
    4. Records for non-consolidated agency IT assets shall be updated by June 1 each year.

B. OIT shall develop, document, and maintain an inventory of consolidated agency IT assets in a system of record designated by OIT. While OIT maintains a centralized IT asset inventory, it is the responsibility of each consolidated agency to provide any additional IT asset inventory information they have available. OIT uses this inventory to complete legislatively mandated reports that provide a statewide perspective of information technology used by state agencies.
    1. OIT shall establish a process for the development and maintenance of the IT asset inventory, including a phased approach for initial inventory population, as appropriate.
    2. Consolidated agencies shall contribute data points required by OIT in the format and according to the timing designated by OIT.
        a. OIT shall approve inventory data before use.

b. The inventory shall include documentation of the connections and relationships between an individual IT asset and other IT assets, when present.

3. IT assets shall be recorded in the system of record designated by OIT.
4. IT assets must be added to the system of record before being connected to the state network or the date they are put in use, whichever occurs first.
5. IT asset records shall be updated by June 30 each year according to the following schedule:
    a. IT assets in tier 0 or 1 for either criticality or risk level - update every year and whenever there is a status change like the announcement of the end of manufacturer support.
    b. IT assets in tier 2 or 3 for criticality and tier 2 for risk level - update every 1 year.
    c. IT assets in tier 3 or 4 for criticality and tier 3 for risk level - update every 2 years.

C. OIT complies with the Colorado Open Records Act (CORA), C.R.S. sections 24-72-200.1, et seq. for all public information requests. The OIT custodian may deny the right of inspection if it is contrary to the public interest, including requests related to security under C.R.S. section 24-72-204 (VIII). OIT may request a decision from the Office of the Attorney General for all public information requests seeking IT asset inventory information where sensitive security information may be involved.

12.6 Reporting

A. On or before November 1 each year, OIT shall deliver an annual report to the Joint Budget Committee (JBC) and Joint Technology Committee (JTC) providing an estimate of the technical debt environment for consolidated agencies.
    1. The report shall evaluate the risks associated with the information technology operating landscape, including IT assets that are out of the acceptable tolerance level for one or more of the tolerance boundaries: information security risk, infrastructure risk, operating cost, productivity cost, and talent depreciation.

2. The report shall include an estimate of the cost associated with upgrading IT assets to the acceptable tolerance level in order to move from a higher risk position to an acceptable risk position.

B. On or before June 15 each year, OIT shall deliver an annual fiscal impact analysis to the Office of State Planning and Budgeting (OSPB) for all state agencies, including consolidated agencies, non-consolidated agencies, and institutions of higher education. The analysis shall detail the current IT assets to which ADLE payments are being applied and the estimated amount of general fund money required to make ADLE payments for the coming fiscal year.

12.7 Compliance

A. A state agency's failure to participate in the inventory of IT assets in compliance with these rules shall be noted in OIT's annual reports to the Office of State Budget Planning (OSPB), the Joint Budget Committee (JBC), and the Joint Technology Committee (JTC) as appropriate.

12.8 Materials Incorporated by Reference

A. The following standards are hereby incorporated by reference into 8 CCR 1501-12, Rule 12.9 Tolerance Boundaries for Consolidated Agencies, pursuant to C.R.S. §24-4-103(12.5), and do not include any later amendments.

1. The Center for Internet Security (CIS) Controls, version 8, released May 2021 incorporated by reference into these rules is available at no cost in an electronic form online at https://learn.cisecurity.org/control-download or from Center for Internet Security, Inc., 31 Tech Valley Drive, East Greenbush, NY 12061.
2. The National Institute of Standards and Technology (NIST) Cybersecurity Framework, version 2.0, published February 26, 2024, incorporated by reference into these rules is available at no cost in an electronic form online at https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-c

sf-20/final or from National Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD 20899.

B. The Colorado Governor's Office of Information Technology also maintains a copy of the policies, rules, and standards incorporated by reference into these rules, which is available from the office during regular business hours.

12.9 Tolerance Boundaries for Consolidated Agencies

Like other physical items, IT assets have a useful lifespan. After a period of time, performance degrades, maintenance costs increase, productivity declines, and repairs and security risks increase. The following boundaries describe the parameters to identify when IT assets exit their optimal functionality and productivity and introduce increased cost and risk.

Non-consolidated agencies may adopt this Rule 12.9 or a similar framework in order to promote consistent state-wide categorization.

The CIS Controls, version 8, released May 2021 and NIST Cybersecurity Framework, version 2.0, published February 26, 2024 are hereby incorporated into the rules by reference, excluding any later amendments.

A. Information Security Tolerances

1. Acceptable
    a. Asset is under manufacturer maintenance and receiving manufacturer updates and service.
    b. Asset conforms to or supports the encryption and security standards established by the National Institute of Standards and Technology (NIST) and Center for Internet Security (CIS) Controls.
2. Marginal
    a. Asset is no longer supported by the manufacturer through no-cost upgrades, however it can be temporarily supported through an extended fee-for-service agreement.
3. Unacceptable
    a. End of manufacturer support, manufacturer no longer providing regular maintenance, support, or updates.

b. Lacks, incompatible or unable to meet the encryption and security standards established by the National Institute of Standards and Technology (NIST) and Center for Internet Security (CIS) Controls.

B. Infrastructure Tolerances

1. Acceptable
    a. Asset exists within, operates, applies, or maintains baseline configurations consistent with the enterprise architecture at the state agency.
    b. Asset is compatible with current and planned connections, relationships, and dependent systems.
2. Marginal
    a. Asset is approaching the end of its useful life within the enterprise architecture at the state agency. Asset must be modernized in accordance with the enterprise architecture to minimize operational impacts to the overall agency ecosystem.
3. Unacceptable
    a. Asset operates on outdated infrastructure.
    b. Asset is incompatible with current and planned connections, relationships, and/or dependent systems.

C. Operating Cost Tolerances

1. Acceptable
    a. Total of manufacturer and supplier costs are less than the depreciated value of the IT asset.
    b. Maintenance support and/or replacement parts available from the manufacturer or supplier.
    c. Currently and consistently obtaining maintenance support according to the manufacturer’s service schedule or service agreement.
    d. No emergency repairs or maintenance conducted.
2. Marginal

a. Cost for manufacturer or supplier service and support agreement is less than the replacement cost but exceeds the current depreciated value of the IT asset.
b. Cost of maintenance exceeds the current depreciated value of the IT asset.
c. Maintenance support and/or replacement parts not available from the manufacturer or supplier.
d. Inconsistently obtaining maintenance support according to the manufacturer's service schedule or service agreement.
e. One emergency repair or maintenance incident in the past year.

3. Unacceptable
    a. Cost for manufacturer or supplier service and support agreement exceeds the replacement cost.
    b. Cost of maintenance exceeds the replacement cost.
    c. Maintenance support and replacement parts are not available from any source.
    d. Not obtaining maintenance support according to the manufacturer's service schedule or service agreement.
    e. Multiple emergency repair or maintenance incidents in the past year.

D. Productivity Cost Tolerances

1. Acceptable
    a. Response time or latency matches historical baseline or industry standards.
    b. Based on load testing, currently operating within performance limits with capacity for additional load.
2. Marginal
    a. Response time or latency lags historical baseline or industry standards by less than 25%.
    b. Based on load testing, currently operating within performance limits; lacks capacity for additional load.
3. Unacceptable

a. Response time or latency lags historical baseline or industry standards by 25% or more.
b. Based on load testing, currently operating at maximum performance limits.
c. Occurrence of errors, timeouts, or failed requests exceeds the historical average for that asset by 20% or more.

E. Talent Depreciation Tolerances

1. Acceptable
    a. Written in a current programming language that is listed among the 2024 average top ten languages in the TIOBE index, which include the following: C, C++, C#, Fortran, Go, Java, JavaScript, Python, SQL, and Visual Basic.
2. Marginal
    a. Written in an older programming language that is still supported by an active community with current documentation.
3. Unacceptable
    a. Written in an obsolete programming language that is not supported by an active community, lacks current documentation, and is not listed among the 2024 average top ten languages in the TIOBE index.

12.10 Classification Tiers for Consolidated Agencies

IT assets are classified based on business criticality and risk level. The classification tiers categorize IT assets based on the cost of an outage and the probability that an outage will occur.

Non-consolidated agencies may adopt this Rule 12.10 or a similar framework in order to promote consistent state-wide classification.

A. Criticality Level

1. Tier 0 - OIT Infrastructure (foundational for Tiers 1 - 4). OIT core infrastructure is the foundational infrastructure that all other tiers depend on to function. The applications in subsequent tiers cannot function without the core

infrastructure in Tier 0. This includes physical data center, firewalls, core network switches/routers, ESX infrastructure, active directory, DHCP, and DNS servers.

2. Tier 1 - Applications and services that, if unavailable, risk human life. For example, law enforcement systems.
3. Tier 2 - Applications and services that, if unavailable for hours, create significant risk for the agency's performance of its designated mission. For example, Salesforce and security video footage.
4. Tier 3 - Applications and services that, if unavailable for days, create significant risk for the agency's performance of its designated mission. For example, state assistance program applications and state permitting systems.
5. Tier 4 - Applications and services that, while not intended to be down for extended periods, do not pose a significant risk to the agency's ability to perform its designated mission. For example, applications used internally like PDF viewers and SharePoint.

B. Risk Level

1. Tier 1 - In the unacceptable risk level for any tolerance boundary, representing a high outage probability.
2. Tier 2 - In the marginal risk level for any tolerance boundary, representing a moderate outage probability.
3. Tier 3 - In the acceptable risk level for all tolerance boundaries, representing a low outage probability.

12.11 IT Lifecycle Management Plan for Consolidated Agencies

A. The IT lifecycle vision for consolidated agencies is to monitor, maintain, and update IT assets within their acceptable tolerance levels and plan for scheduled and orderly replacement to decommission IT assets before they reach unacceptable tolerance levels.

B. IT assets at consolidated agencies that are outside of the acceptable tolerance boundaries may be prioritized for replacement based on criticality and risk to avoid future and further obsolescence.

C. Due to the risks they present, IT assets at consolidated agencies that operate outside of the acceptable tolerance levels may be subject to actions to mitigate the risks or reduce vulnerabilities, as determined by the OIT Chief Information Officer or delegate, until they are upgraded to the acceptable tolerance level. Actions could include but are not limited to:
    1. Limited connections to other IT assets
    2. Limited user accounts
    3. Limited feature updates
    4. Temporary or permanent freeze on changes or updates
    5. Temporary or permanent suspension or discontinuation
D. Affected agencies will be notified and consulted to determine risk mitigation actions, replacement needs, assessment, procurement, and scheduling.
E. Non-consolidated agencies may adopt this Rule 12.11 or develop similar IT lifecycle management plans for their respective state agencies.

12.12 Appeals and Exceptions for Consolidated Agencies

A. A consolidated agency may dispute an action taken under these rules by submitting a written appeal through the agency's IT Director to the OIT Chief Information Officer (OIT CIO). The OIT CIO or delegate shall deliver a written decision within 30 calendar days to uphold, modify, or reverse the action.
B. In exceptional circumstances, a consolidated agency may request a temporary exception to these rules if it can demonstrate that compliance would result in undue hardship or significant operational challenges. Exception requests must be submitted in writing through the agency's IT Director to the OIT CIO, and must include:
    1. A detailed explanation of the circumstances necessitating the exception.
    2. Evidence of the undue hardship or significant operational challenges that would arise from compliance.
    3. A proposed alternative solution that addresses the risks associated with non-compliance.
    4. A timeline for implementing the proposed alternative solution and achieving compliance with the rules.

C. The OIT CIO or delegate will review exception requests on a case-by-case basis and may grant exceptions if they are deemed necessary and appropriate. Granted exceptions may be temporary or subject to specific conditions or limitations, and will be reviewed periodically to ensure they remain justified and aligned with the overall goals of the rules.

D. In the event a dispute arises between a consolidated agency and OIT in relation to these rules, the OIT CIO and the Agency's Executive Director will attempt to resolve the dispute. If the OIT CIO and the Agency's Executive Director are unable to resolve the dispute within ten (10) business days from the date the dispute arises, then the dispute shall be referred to the Governor for final resolution.

12.13 Severability

If any provision of these Colorado Information Technology Lifecycle Planning Rules, 8 CCR 1501-12, is found to be invalid by a court of competent jurisdiction, the remaining provisions of these rules shall remain in full force and effect.