Minnesota IT Services: Cloud-Based Information Technology Services

Performance Audit

March 2026

Financial Audit Division

The division has authority to audit organizations and programs in the state's executive and judicial branches, metropolitan agencies, several "semi-state" organizations, state-funded higher education institutions, and state-funded programs operated by private organizations.

Each year, the division selects several of these organizations and programs to audit. The audits examine the policies and procedures—called internal controls—of the organizations to ensure they are safeguarding public resources and complying with laws that govern their financial and program operations. In addition, the division annually audits the State of Minnesota's financial statements and the financial statements of three state public pension systems. The primary objective of these financial audits is to assess whether the statements fairly present the organization's financial position according to Generally Accepted Accounting Principles.

OLA has two additional divisions. The Program Evaluation Division determines the extent to which state agencies and programs have met their goals and objectives, and used resources efficiently. OLA's Special Reviews Division investigates allegations of wrongdoing within state government.

For more information about OLA and to access reports and report updates, go to: www.auditor.leg.state.mn.us.

March 24, 2026

Members
Legislative Audit Commission

Jon Eichten, Commissioner and Chief Information Officer
Minnesota IT Services

This report presents the results of our performance audit of select cloud-based information technology (IT) services managed by Minnesota IT Services (MNIT). The objectives of this audit were to determine if MNIT had adequate internal controls over selected activities, followed best practices, and complied with significant requirements.

This audit was conducted by Mark Mathison, CISA, CISSP, CPA Inactive (IT Audit Director); and IT auditors Deb Frost, CISA; Rob Riggins, CISA, CISSP; and Peng Xiong.

We received the full cooperation of MNIT staff while performing this audit.

Sincerely,

Judy Randall
Legislative Auditor

Lori Leysen, CPA
Deputy Legislative Auditor

OLA

Table of Contents

OLA

Introduction

Minnesota IT Services (MNIT) is the State of Minnesota's central information technology organization. It is responsible for building, maintaining, and securing the executive branch's information technology (IT) infrastructure, applications, projects, and services.

Auditors focus on internal controls as a key indicator of whether an organization is well managed. Internal controls are the policies and procedures management establishes to govern how an organization conducts its work and fulfills its responsibilities. A well-managed organization has strong controls across all of its internal operations. If effectively designed and implemented, controls help ensure, for example, that inventory is secured, computer systems are protected, laws and rules are complied with, and authorized personnel properly document and process financial transactions.

> **Minnesota Law Mandates Internal Controls in State Agencies**
>
> State agencies must have internal controls that:
>
> - Safeguard public funds and assets and minimize incidences of fraud, waste, and abuse.
>
> - Ensure that agencies administer programs in compliance with applicable laws and rules.
>
> The law also requires the Commissioner of Minnesota Management and Budget to review OLA audit reports and help agencies correct internal control problems noted in those reports.
>
> **— *Minnesota Statutes* 2025, 16A.057**

In this audit, we focused on cloud computing services that MNIT makes available to executive branch agencies.[1] In particular, we examined whether MNIT appropriately awarded contracts for primary cloud services; accurately recorded cloud-related inventories, costs, and expenditures in compliance with state laws and policies; and adequately reported the progress of executive branch cloud adoption to the Legislature.

---

[1] *Minnesota Statutes* 2025, 16E.03, subd. 1(g), defines cloud computing as the meaning described by the National Institute of Standards and Technology of the U.S. Department of Commerce in Special Publication 800-145 (September 2011). We explain cloud computing in more detail on page 5 of this report.

OLA

Report Summary

Conclusion

Minnesota IT Services generally complied with the criteria we tested. We identified only one issue related to legislatively required cloud progress reporting.

Finding and Recommendation

Finding. Minnesota IT Services did not include Microsoft Azure support and maintenance costs in its cloud progress reports. (p. 21)

Recommendation

Minnesota IT Services should include all cloud-related support and maintenance costs in future cloud progress reports.

OLA

Background

Minnesota IT Services

Minnesota IT Services (MNIT) is the information technology (IT) department for Minnesota's executive branch. Led by the state's chief information officer, MNIT sets IT strategy, direction, policies, and standards for Minnesota state agencies, boards, councils, and commissions.

MNIT purchases most IT-related goods and services on behalf of Minnesota's executive branch agencies and delivers two main types of IT services, as detailed below.

(1) MNIT staff, working within the respective state agencies, develop and support agency-specific applications and projects.

(2) MNIT provides centralized services, such as email; desktops; telephone services; networking; security; and infrastructure services, including "the cloud"; across the executive branch.

Our audit focused on cloud computing services available to executive branch agencies.

Cloud Computing

Cloud computing ("the cloud") is the on-demand availability of computing resources (for example, application development tools, data storage, networking capabilities, servers, and software) over the internet.[2] For many cloud computing services, customers (individual users) use their internet browser and cloud management tools to activate computing resources when they are needed, and then shut them off when they are no longer needed. This flexibility is possible because a cloud provider pools computing resources to serve multiple customers, or "tenants," using a multi-tenant model. In this type of model, different physical and virtual resources are dynamically assigned and reassigned according to customer demand. Cloud service providers, such as Amazon Web Services (AWS) or Microsoft Azure (Azure), group these pooled resources into a category of computing service (for example, processing, storage, network) and measure how much a customer uses of the service using a meter, much like an electric meter in a home. Customers typically pay only for the cloud services they use.[3]

When organizations use these shared computing resources, they are able to provide IT services at a lower cost because upfront investment, maintenance, and excess capacity

---

[2] National Institute of Standards and Technology, *NIST Special Publication 800-145: The NIST Definition of Cloud Computing* (September 2011). Appendix A of this report provides additional terminology related to cloud computing.

[3] Cloud service providers offer several pricing models that let organizations choose how they want to pay for resources. This flexibility helps organizations manage costs more efficiently based on their workload patterns, budgets, and performance needs. Common pricing models include Pay-As-You-Go, Reserved Instances, and Spot Virtual Machines/Spot Instances.

costs can be shared across multiple customers in the cloud.[4] With the combined flexibility of on-demand access and the ability to take advantage of the cloud provider's existing expertise in new and different services, organizations can also more quickly deliver IT services and improve customer service. For example, rather than purchasing computer hardware and software that organizations need to install within their own data centers, organizations can more quickly purchase and use cloud services, such as email or on-line storage services to back up files and data.

Cloud service providers offer different service models. A cloud service model refers to the type of computing services delivered in the cloud. There are three primary service models available: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).[5] Each service model offers customers an increasing level of computing resources that are managed by the cloud provider, as shown in Exhibit 1. This audit focused on MNIT's IaaS and PaaS models.

Exhibit 1
Common Service Models in Cloud Computing
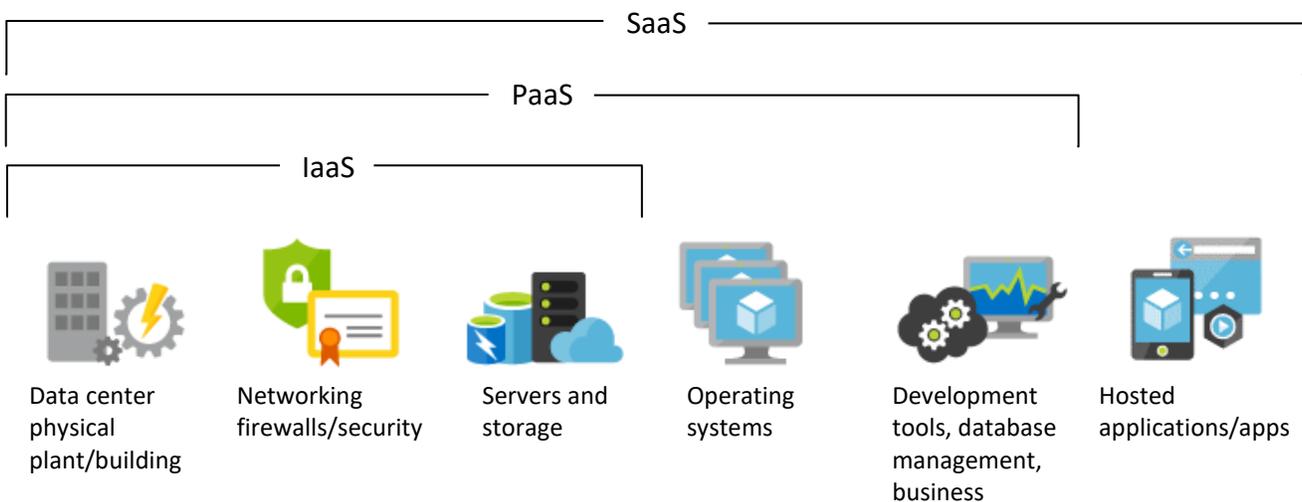
Source: Office of the Legislative Auditor, based on "Software as a Service (SaaS)," U.S. General Services Administration, Cloud Information Center, accessed August 18, 2025, https://cic.gsa.gov/solutions/saas/.

---

[4] National Institute of Standards and Technology, *NIST Special Publication 800-146: Cloud Computing Synopsis and Recommendations* (May 2012), Chapter 7, p. 5. Capacity planning focuses on how well a system can execute tasks under varying loads. During peak performance, additional computing speed, memory, storage, and network throughput are needed to ensure systems can process data quickly and efficiently.

[5] With **IaaS**, the service provider delivers and manages the basic computing infrastructure of servers, software, storage, and network equipment. The consumer provides the operating system, programming tools and services, and applications. With **PaaS**, the service provider delivers and manages the infrastructure, operating system and programming tools and services, which the consumer can use to create applications. With **SaaS**, the service provider delivers one or more applications and all of the resources (operating system and programming tools) and underlying infrastructure to run them for use on demand. National Institute of Standards and Technology, *NIST Special Publication 800-145: The NIST Definition of Cloud Computing* (September 2011).

MNIT and Cloud Services

MNIT has used cloud services for nearly 15 years. In 2010, Minnesota began an initiative to move almost 40,000 workers in more than 70 agencies to Microsoft Office 365 (Microsoft 365), a cloud solution for email and collaboration tools. MNIT's increased reliance on cloud services has continued through 2025 with expanding services and scope.[6] A primary effort for better utilizing cloud services, and the focus for this audit, is MNIT's Cloud Readiness and Modernization Project (CloudRAMP).

CloudRAMP is a multiyear project, which began in 2021, to better prepare the state's IT infrastructure for cloud adoption and modernization. MNIT describes its CloudRAMP strategy as an intentional cloud approach, using a variety of cloud service providers. Under this approach, MNIT selects a primary cloud service provider for delivering key IT services, with the goal of reducing support costs and improving efficiency, institutional knowledge, and service delivery for specific technologies.[7] Other IT services can take advantage of innovative solutions from different, or secondary, cloud providers. This intentional use of blended cloud-based services is known as a "multicloud strategy."[8]

> A multicloud strategy is "the deliberate use of cloud services from multiple public cloud providers for the same general class of IT solutions or workloads."
>
> **— Information Technology Glossary: Multicloud Strategy**

During our audit, MNIT managed IaaS and PaaS assets with three cloud providers: AWS, Azure, and Google Cloud.[9] Azure is designated as the primary cloud provider.

This multicloud approach allows MNIT and its agency partners to leverage the strengths of different cloud platforms, ensuring they can select the best tools for specific workloads and applications. For instance, an agency might use AWS for its computing needs while relying on Azure for application development and Google Cloud for language translation services.

There are several benefits of using a multicloud strategy, such as:

Avoiding Vendor Lock-In: By spreading services across multiple providers, MNIT can reduce its dependency on a single vendor, allowing for greater flexibility and negotiating power.

Optimizing Performance: Different cloud providers may excel in various areas, such as machine learning, storage, or geographic availability. A multicloud approach enables MNIT to choose the best service for each specific requirement.

---

[6] Appendix B of this report provides a timeline of MNIT's history with the cloud.

[7] Minnesota IT Services, "Minnesota's Executive Branch Cloud Strategy," April 2023.

[8] "Information Technology Glossary: Multicloud Strategy," Gartner, accessed January 31, 2025, https://www.gartner.com/en/information-technology/glossary/multicloud-strategy.

[9] MNIT used Google Cloud to support one agency application.

Enhancing Resilience: Utilizing multiple cloud services can improve operational resilience by distributing workloads. This helps mitigate risks associated with service outages or data loss from a single provider.

Cost Efficiency: MNIT can select the most cost-effective services for its needs, potentially leading to significant savings. This flexibility can also enhance the ability to negotiate competitive pricing with providers.

On the other hand, implementing a multicloud strategy can introduce certain challenges that MNIT needs to consider. These include:

Complexity in Management: Managing multiple cloud environments can be complex, requiring robust governance and management tools to ensure seamless integration and operation across platforms.

Data Security and Compliance: Ensuring consistent security measures and compliance with regulations across different cloud providers can be challenging.

Interoperability Issues: Applications and services from different providers may not always work well together, necessitating careful planning and integration efforts to ensure smooth operation.

Cloud Financial Management

Traditional IT services, where organizations run computer hardware and software in data centers they manage, typically involve upfront purchases of the hardware, software, and data centers that depreciate over the asset's useful life. The purchase process often requires significant planning and a lengthy approval process. To minimize the number of delays, organizations often need to purchase and install computing resources based on the highest expected capacity—such as the highest number of expected system users—often leaving resources underutilized during low-demand periods. For example, a government organization that is generally busy once per year with an annual submission of documents, would need to purchase IT resources for high expected usage occurring just once a year. Further, in many cases it would need to replicate those resources to have separate testing and development environments.

In contrast, cloud-based services operate under a consumption-based model, or variable cost model, whereby the government organization pays for what it uses when it is needed. So, rather than purchasing hardware and software for peak performance occurring once a year, cloud-based services allow the government organization to run its application using a lower tier of services throughout the year, and "rent" additional capacity for its peak-performance periods.

When organizations shift to this variable usage of IT resources, accounting practices also need to shift to better predict and manage cloud spending. New financial management strategies have emerged to help solve this challenge, collectively referred to as FinOps.[10] Recognizing the need for these new practices, MNIT included processes within CloudRAMP to implement and improve FinOps practices. Exhibit 2 shows one example of how MNIT's new FinOps tools help monitor Azure costs and can assist with detecting anomalies or deviations in spending patterns.

Exhibit 2

Example of MNIT's Cloud Cost Monitoring (FinOps)

$1,486,788 Prior Month Cost
$173,205 Current Month Cost
$49,117 Average Daily Cost in the Last 30 Days

Cost by Day   **Granularity:**   Day   Month   Year
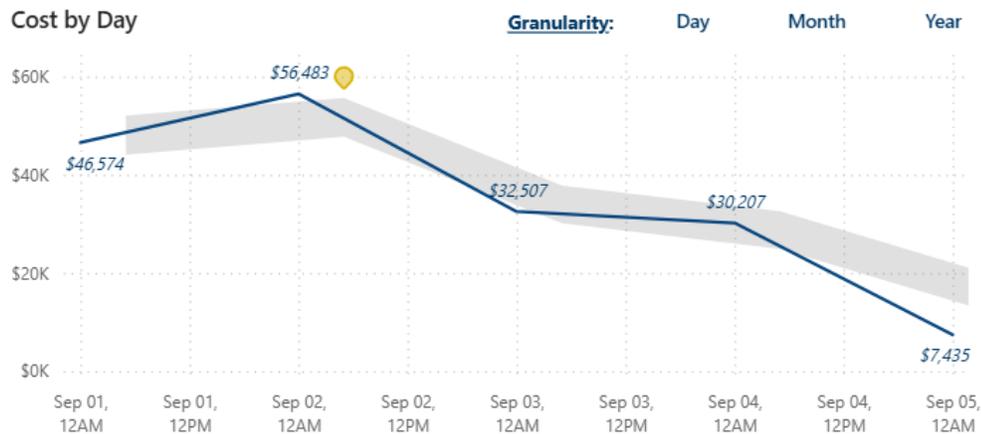
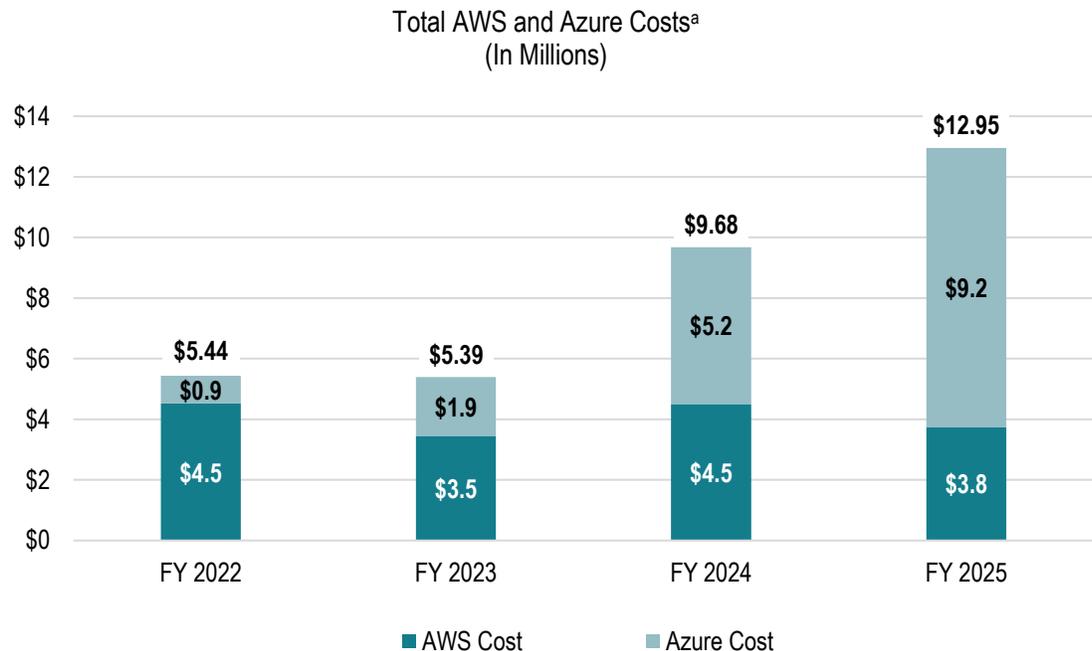Source: MNIT's FinOps reporting tools, as of September 5, 2025.

MNIT's FinOps tools currently track IaaS and PaaS costs affiliated with AWS and Azure, which are a subset of the cloud expenditures recorded in the state's accounting system. MNIT reported over $55 million in cloud-related purchases for Fiscal Year 2024.[11] Payments for AWS and Azure—the state's two largest IaaS and PaaS service providers—accounted for $9.7 million, just over 17 percent of MNIT's total cloud-based expenditures in Fiscal Year 2024.

Exhibit 3 illustrates how MNIT's AWS and Azure usage costs have more than doubled over the past four fiscal years. Using its FinOps tools, and detailed usage and cost data obtained from each cloud provider, MNIT can actively monitor and track usage of cloud resources within AWS and Azure. These tools enable MNIT to monitor and report usage and costs by agency, resource, and a variety of other attributes. With FinOps, MNIT can be transparent about how it bills each agency based on the agency's AWS and Azure usage.

---

[10] "What Is FinOps?", FinOps Foundation, accessed April 25, 2025, https://www.finops.org/introduction /what-is-finops/.

[11] Minnesota IT Services, *MNIT Legislative Report—Cloud Progress Report* (January 2025), 1. These data include IaaS, PaaS, and SaaS expenditures but exclude MNIT's Office 365 costs for its communication and collaboration suite. Most of MNIT's cloud spending was associated with SaaS.

**MNIT's Cloud-Based Expenditures for AWS and Azure,
Fiscal Years 2022 Through 2025**

Total AWS and Azure Costs[a]
(In Millions)

[a] Azure costs do not include amounts paid to Microsoft for support service plans.

Source: Office of the Legislative Auditor, based on data from the state's accounting system and MNIT's FinOps reporting tools.

Cloud Transformation Appropriation

In 2023, the Legislature appropriated $33.6 million to MNIT to implement modern and improved digital, cloud-based applications and services.[12] These funds were not intended to pay for ongoing cloud usage expenses. MNIT used most of these funds to obtain professional/technical services from a variety of contractors to assist with modernizing and migrating its information technology infrastructure and applications to cloud platforms. Exhibit 4 shows how MNIT used this appropriation through Fiscal Year 2025, and how it plans to use the remaining funds for fiscal years 2026 and 2027.

> MNIT received a onetime appropriation of $33.6 million to support planning, migration, infrastructure, training, and services required for executive branch cloud transformation.
>
> — *Laws of Minnesota* **2023, chap. 62, art. 1, sec. 10(c)**

---

[12] *Laws of Minnesota* 2023, chapter 62, art. 1, sec. 10(c). These funds are available until June 30, 2027.

Exhibit 4

MNIT's Cloud Transformation Expenditures and Budget, as of June 30, 2025

Description	FY 2024 Expenditures	FY 2025 Expenditures	FY 2026 Budget	FY 2027 Budget	Total
Full-Time Salaries	$ 206,084	$ 395,926	$ 640,000	$ 188,000	$ 1,430,010
Overtime and Premium Pay	–	122,830	125,000	125,000	372,830
IT Professional and Technical Services	5,641,418	8,358,896	10,277,154	729,086	25,006,554
Computer and System Services	1,462,971	3,063,414	1,138,103	1,039,483	6,703,971
Total	**$7,310,473**	**$11,941,066**	**$12,180,257**	**$2,081,569**	**$33,513,365**

Note: MNIT had not budgeted $81,635 of its appropriation.

Source: Office of the Legislative Auditor, based on data from the state's accounting system and MNIT's FinOps reporting tools.

MNIT developed a four-year plan to use its appropriation to achieve four goals: (1) migrate at least 70 percent of executive branch on-premises servers to the cloud, (2) establish standardized, modern, cloud-oriented processes for software development and information technology operations teams, (3) provide training and staff development resources, and (4) become elite at cloud financial management practices (FinOps).[13] MNIT has established budgets to track its expenditures for each of these goals. Exhibit 5 shows the budgets and expenditures, through June 30, 2025, for each goal.

Exhibit 5

MNIT's Budget and Use of Cloud Transformation Funding by Goal, as of June 20, 2025

Goal	Total Budget Amount FY2024 Through FY2027	Total Expenditures FY2024 Through FY2025	Percentage of Budget Spent
Goal 1: Migrate On-Premise Servers to Cloud	$29,598,270	$17,397,126	58.8%
Goal 2: Modern Development and Operational Processes	2,460,777	1,267,695	51.5%
Goal 3: Training and Staff Development	605,779	498,079	82.2%
Goal 4: Elite Cloud FinOps	848,539	88,639	10.4%
Total	**$33,513,365**	**$19,251,539**	**57.6%**

Note: MNIT has not budgeted $81,635 of its appropriation.

Source: Office of the Legislative Auditor, based on data from the state's accounting system and MNIT's FinOps reporting tools.

---

[13] Minnesota IT Services, *2023 Annual Report: Moving to the Cloud: CloudRAMP*, https://mn.gov/mnit/assets/MNIT%20Annual%20Report%202023%20FINAL%20-%20web_tcm38-609375.pdf, 20, accessed January 27, 2025. As of October 2022, only 5 percent of executive branch servers were in the cloud. Minnesota Management and Budget, *Revised 2024–25 Governor's Biennial Budget Recommendations, Minnesota IT Services* (March 2023), 15.

Progress in Cloud Adoption

The 2023 Legislature established a new requirement for MNIT to annually report on the progress the executive branch has made in cloud adoption.[14] The law requires MNIT to report—at a minimum—on cloud-related expenditures and current projects that incorporate cloud computing solutions.

In its January 2025 progress report, MNIT reported that it had partnered with 390 cloud providers in Fiscal Year 2024, spending more than $55 million for all IaaS, PaaS, and SaaS. These amounts generally represent the licensing and usage expenses associated with cloud-related operating costs. Additionally, MNIT reported over 180 executive branch IT projects in development that incorporated cloud computing solutions.[15] When compared to cloud activities reported in its January 2024 progress report, MNIT's cloud activities increased. In the 2024 progress report, MNIT reported that it had partnered with 307 cloud providers in Fiscal Year 2023, spent more than $33.5 million for all IaaS, PaaS, and SaaS, and had worked on just over 150 executive branch IT projects that incorporated cloud computing solutions.[16]

Exhibit 6 depicts how IT cloud-based projects rely on a variety of cloud-based providers. For example, MNIT may have one IT project migrating from an on-premise data center to AWS or Azure environments, while another project utilizes some components of Salesforce technologies in conjunction with Formstack on-line forms and electronic signature capabilities found within DocuSign.

Exhibit 6

Example of IT Projects Interacting with Cloud-Based Providers
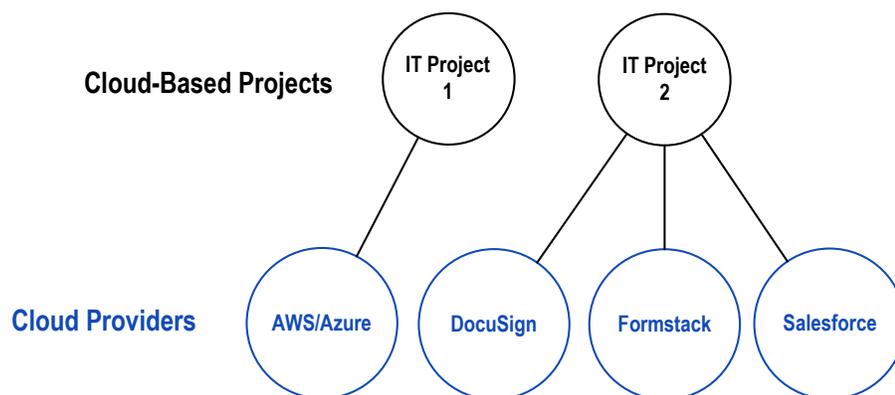
Source: Office of the Legislative Auditor.

---

[14] *Laws of Minnesota* 2023, chapter 62, art. 6, sec. 12, codified as *Minnesota Statutes* 2025, 16E.03, subd. 5a.

[15] Minnesota IT Services, *MNIT Legislative Report—Cloud Progress Report* (January 2025). These numbers include IaaS, PaaS, and SaaS expenditures but exclude MNIT's Office 365 costs for its communication and collaboration suite. MNIT managed a total of 403 IT projects in Fiscal Year 2024, indicating that roughly 45 percent of its projects incorporated cloud computing solutions. MNIT's January 2026 Cloud Progress Report indicates an additional increase in cloud-related expenditures (a total of $78 million) and an increase in the number of cloud providers (453). Minnesota IT Services, *MNIT Legislative Report—Cloud Progress Report* (January 2026).

[16] Minnesota IT Services, *MNIT Legislative Report—Cloud Progress Report* (January 2024).

As noted in Exhibit 3 (page 10), while AWS costs have stayed fairly consistent, MNIT's cloud-based expenditures for Azure have increased from $0.9 million in Fiscal Year 2022 to $9.2 million in Fiscal Year 2025. The increase in cost directly correlates with the growth of computing resources within the Azure environment. As shown in Exhibit 7, usage of virtual machines within MNIT's Azure environment increased from 12 servers on July 1, 2021, to over 1,300 servers on April 30, 2025.[17] The thicker lines in Exhibit 7 indicate that MNIT has a larger range of virtual machines operating within a given day. This range is due to MNIT activating virtual machines when they are needed and shutting them down—conserving resources and reducing costs—when they are not needed. For example, on weekends, MNIT can shut down virtual machines that are generally only needed Monday through Friday; similarly, MNIT can shut down computing resources during daytime hours for virtual machines only needed for overnight batch processing.

Exhibit 7

**Use of Virtual Machines Within MNIT's Azure Environment,
July 1, 2021, Through April 30, 2025**

Number of Virtual Machines
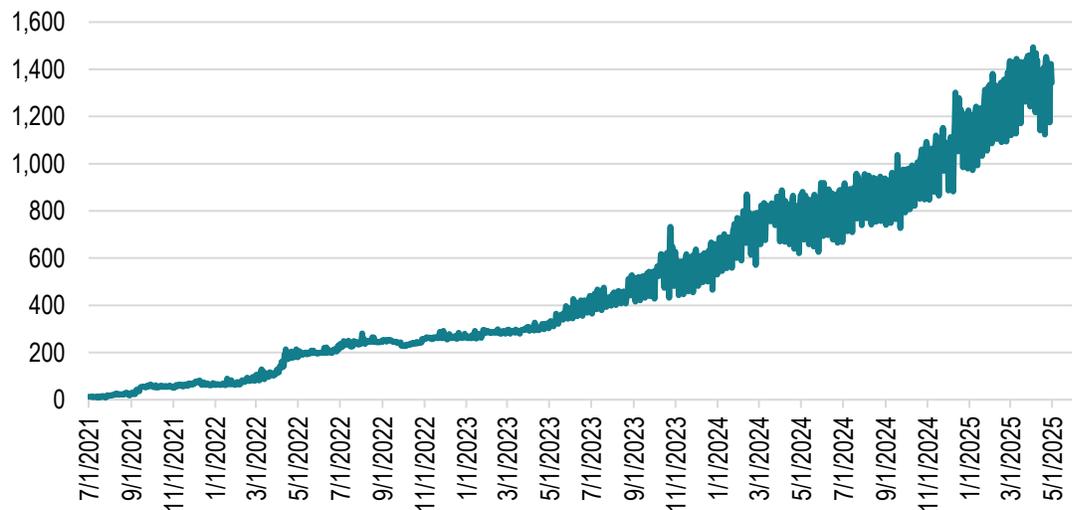
Source: Office of the Legislative Auditor, based on data from MNIT's FinOps reporting tools.

As MNIT moves more of its computers to the cloud, the need to manage these resources within state-run data centers decreases. Recognizing this, MNIT announced that it plans to close one of its primary leased data centers by September 30, 2027.[18]

---

[17] Virtual machines are one of several types of on-demand, scalable computing resources that Azure offers. Virtual machines (virtual servers and virtual desktop computers) give organizations the flexibility of having access to computing devices without having to buy and maintain the physical hardware.

[18] Minnesota IT Services, *Q1 2025 Quarterly Report* (May 2025), 16.

OLA

Audit Scope, Objectives, and Methodology

We conducted this audit to determine whether Minnesota IT Services (MNIT) complied with the requirements we tested. The audit scope included cloud-related Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) procurement, asset inventory, cost monitoring, payments, and progress reporting. In particular, we focused our efforts on cloud resources within Microsoft Azure (Azure) and Amazon Web Services (AWS). The period under examination was from July 1, 2021, through June 30, 2025.

We conducted this performance audit in accordance with generally accepted government auditing standards.[19] Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. When sampling was used, we used a sampling method that complies with generally accepted government auditing standards and that supports our findings and conclusions. That method does not, however, allow us to project the results we obtained to the populations from which the samples were selected.

We assessed internal controls against the internal control standards published by the U.S. Government Accountability Office.[20] To identify compliance criteria for the audit, we examined state laws; state contracts; policies, procedures, and standards established by Minnesota Management and Budget, the Department of Administration, and MNIT; and cloud-related best practices established by the FinOps Foundation, National Institute of Standards and Technology, and the Center for Digital Government.[21]

Cloud Procurement

MNIT performs most IT-related procurement on behalf of Minnesota's executive branch agencies. In November 2020, MNIT issued a request for proposals (RFP) seeking to select its primary vendor to provide cloud hosting and services related to IaaS and PaaS.[22] Five vendors responded to the RFP, and Microsoft Azure received the final award.

---

[19] Comptroller General of the United States, Government Accountability Office, *Government Auditing Standards, 2018 Revision* (Washington, DC, Technical Update April 2021).

[20] Comptroller General of the United States, Government Accountability Office, *Standards for Internal Control in the Federal Government* (Washington, DC, September 2014). In September 2014, the State of Minnesota adopted these standards as its internal control framework for the executive branch.

[21] Appendix C details the specific compliance requirements we tested.

[22] A request for proposals (RFP) is a formal invitation to potential contractors or grantees to submit a proposal. Proposals should identify how potential contractors or grantees will respond to the needs or requirements outlined within the RFP.

As part of our review of the RFP process, we examined solicitation and contract management activities, including proposal development, response management, proposal evaluation and award, and contract negotiations and amendments. We also examined MNIT contracts for AWS as MNIT's second largest vendor for cloud IaaS services.

We designed our work to determine whether MNIT complied with the Department of Administration Office of State Procurement requirements and best practices for selecting and contracting with cloud providers (as listed in Appendix C).[23] Exhibit 8 lists the areas we tested related to the primary cloud provider RFP solicitation process and cloud contract management requirements, our methodology for testing those areas, and the results of our tests.

Exhibit 8

Cloud Procurement: Area Tested, Testing Methodology, and Result

Area Tested	Testing Methodology	Result
Procurement Policies and Procedures	We reviewed policies and procedures to determine that management documented purchasing control expectations.	No issues.
Request for Proposals (RFP) Development	We inspected all RFP documents provided to participating vendors for compliance with Office of State Procurement (OSP) requirements.	No issues.
RFP Evaluation and Award	We inspected all RFP evaluation and award process documents for compliance with OSP requirements.	No issues.
RFP Negotiation	We reviewed MNIT's negotiation process and inspected all documents related to Microsoft-negotiated discounts, customer investment funding, and other services to validate that best practice negotiations were followed.	No issues.
Cloud Services Contracts	We inspected terms and conditions within seven cloud provider and value-added reseller contracts related to AWS and Azure services for adherence with cloud-specific best practices. Additionally, we inspected related contracts and amendments awarded to Microsoft for compliance with OSP requirements.	No issues.
Risk Authorization and Management Program (RAMP)[a]	We confirmed FedRAMP authorization status for all five RFP responders and reviewed RAMP best practices for the two value-added resellers.[b]	No Issues.

[a] RAMPs are used to ensure the security and compliance of information systems in cloud service model contracting and monitoring using controls based on National Institute of Standards and Technology, *NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations* (September 2020).

[b] "FedRAMP authorized" is a designation provided to cloud service providers by the federal government that indicates an approved third-party organization has assessed and attested to the security capabilities of the cloud service offered. It includes review and acceptance by the FedRAMP Project Management Office.

Source: Office of the Legislative Auditor.

---

[23] The Office of State Procurement, a division within the Minnesota Department of Administration, is the state's central procurement office. Contracts related to Microsoft Azure and AWS include contracts signed directly with the cloud service providers and contracts signed with value-added resellers that provide cloud services, volume discounts, or other services.

Cloud Asset Inventory

Asset management is the process of procuring, tracking, maintaining, and disposing of an asset owned by an organization. While asset tracking typically focuses on an asset's existence, valuation, and location, inventories of IT assets include several additional attributes related to technical, operational, security, and cost management requirements. IT Asset Management (ITAM) allows an organization to monitor and protect its IT assets while preventing unauthorized assets from entering the environment. ITAM supports cloud governance and operational goals by enforcing naming, tagging, and labeling requirements used to allocate costs and optimize operations.[24] For example, MNIT tags its cloud assets with a cost center identifier, which allows it to allocate the cost to a specific state agency, application, or central service.

We designed our work to determine whether MNIT maintained accurate, complete, and consistent inventories of cloud assets in compliance with the criteria we tested (as listed in Appendix C). Exhibit 9 lists the areas we tested related to cloud asset inventory, our methodology for testing those areas, and the results of our tests.

Exhibit 9

Cloud Asset Inventory: Area Tested, Testing Methodology, and Result

Area Tested	Testing Methodology	Result
Inventory Policies and Procedures	We reviewed policies and procedures to determine that MNIT had documented internal controls related to cloud inventory and asset management.	No issues.
Inventory Accuracy	We examined and reconciled a judgmental sample of 15,136 invoiced Azure virtual machine and storage device records to inventory records.	No issues.
Inventory Tagging Requirements	We tested all 37,270 Azure accounting tags, as of March 14, 2025, for completeness and reasonable consistency with the asset's purpose.	No significant issues.
Inventory Naming Requirements	We examined all 1,353 Azure virtual machine records, as of April 30, 2025, for consistency by evaluating the construction and validity of server name attributes.	No significant issues.

Source: Office of the Legislative Auditor.

---

[24] IT tags are a special type of metadata that are customized by an organization. They are used to label and categorize IT resources based on criteria relevant to the organization, such as environment, project, cost center, or ownership.

Cloud Cost and Usage Data, Monitoring, and Anomaly Detection

Cloud costs are based on a consumption model, meaning customers pay based on what they use, much like how a utility company operates. When someone uses electricity, a meter records how much electricity is being used. Similar to electricity, cloud providers determine how much a customer uses each cloud resource with a "meter." Customers are charged based on the meter usage and price per unit, or "rate." Unlike electricity, there are thousands of unique cloud services, each with a different rate. Cloud service providers record each of these services separately based on the specific amount of computing power, memory, storage, and network resources used.

This change from traditional fixed IT costs to actual usage means that monthly cloud bills can fluctuate significantly based on various workload factors, such as time of day, day of the week, scheduled events (such as fiscal reporting periods), or even seasonal usage patterns. MNIT uses specialized cost-monitoring tools to understand, monitor, and report on cloud costs in an attempt to quickly detect and manage unexpected increases in price, usage, or other costs. MNIT's finance team monitors and reports AWS and Azure costs in centralized FinOps tools.

We designed our work to determine whether MNIT's cloud cost and usage data were accurate, and whether MNIT monitored, reported, and used these data to detect unexpected changes in costs in compliance with the criteria we tested (as listed in Appendix C). Exhibit 10 lists the areas we tested related to the cloud cost data, our methodology for testing those areas, and the results of our tests.

Exhibit 10

Cloud Cost and Usage Data, Monitoring, and Anomaly Detection: Area Tested, Testing Methodology, and Result

Area Tested	Testing Methodology	Result
Policies and Procedures	We examined the extent to which MNIT implemented the FinOps Framework's best practices in its FinOps tools to record, monitor, and detect anomalies in usage and costs data.	No significant issues.
Pricing Data Accuracy	Using a judgmental sample, we examined and recalculated the accuracy of pricing data for 78,545 Azure virtual machines and storage records, including volume pricing discounts.	No issues.
Cost and Usage Data Accuracy	Using a judgmental sample, we examined and recalculated the accuracy of: • 390,185 AWS and Azure virtual machine and storage costs, and usage records. • 157 records of purchased discounts for reserved instances, savings plans, and spot instant usage in the Azure cloud.	No issues.
Cost Monitoring and Anomaly Detection	We inspected MNIT's FinOps tools and processes for adherence to FinOps best practices.	No significant issues.

Source: Office of the Legislative Auditor.

Cloud Expenditures

MNIT pays cloud-related expenditures using the state's accounting system. Additionally, MNIT monitors and reports cloud expenditures within its FinOps tools. These dashboards and reports provide comprehensive financial tracking and analysis of aggregated cost trends; compare consolidated invoices submitted by value-added resellers to aggregated AWS and Azure portal usage data and approved purchase order amounts; summarize cost allocations; and forecast future aggregated costs.

We designed our work to determine whether MNIT (1) followed prescribed policies and practices when making payments for AWS and Azure resources (as listed in Appendix C) and (2) accurately paid and recorded expenditures in both the state's accounting system and its FinOps tools. Exhibit 11 lists the areas we tested related to the cloud cost data, our methodology for testing those areas, and the results of our tests.

Exhibit 11

Cloud Expenditures: Area Tested, Testing Methodology, and Result

Area Tested	Testing Methodology	Result
Policies and Procedures	We reviewed policies and procedures to validate that management had documented internal controls related to its accounts payable process.	No issues.
Approval	We sampled and tested 17 of 153 monthly AWS and Azure invoices, including 1 judgmental and 16 random samples, for compliance with MNIT's invoice approval process.	No issues.
Prompt Payment	We sampled and tested 17 of 153 monthly AWS and Azure invoices, including 1 judgmental and 16 random samples, for compliance with state prompt payment requirements.	No significant issues.
Reconciliation	We sampled 17 of 153 monthly AWS and Azure invoices, including 1 judgmental and 16 random samples, and tested the accuracy of MNIT'S invoice reconciliation process.	No issues.
Expenditure Reporting	We sampled 17 of 153 monthly AWS and Azure invoices, including 1 judgmental and 16 random samples, and tested the accuracy of expenditures recorded in the state's accounting system.	No issues.
Data Accuracy	We reconciled all budget and expense data tracked in MNIT's FinOps tools to the state's accounting system.	No issues.
Use of Appropriation	We examined cloud transformation expenditures for unreasonable uses (for example, supplementing operational budgets).	No issues.

Source: Office of the Legislative Auditor.

Cloud Progress Reporting

As mentioned previously, the 2023 Legislature established a new requirement for MNIT to annually report on the progress of executive branch cloud adoption.[25]

We designed our work to determine whether MNIT complied with reporting requirements (as listed in Appendix C) and that the reports contained accurate information. Exhibit 12 lists the areas we tested related to cloud progress reporting, our methodology for testing those areas, and the results of our tests.

Exhibit 12

Cloud Progress Reporting: Area Tested, Testing Methodology, and Result

Area Tested	Testing Methodology	Result
Cloud Reporting Submissions	We tested the timeliness of two annual report submissions to the Legislature.	No issues.
Cloud-Related Expenditures	We tested the accuracy of all 23 reported Fiscal Year 2024 cloud provider expenditures over $500,000 by comparing reported amounts to expenditures recorded within the state's accounting system.	See finding.
Cloud Projects	Using a judgmental sample, we tested the accuracy of 25 of 183 Fiscal Year 2024 cloud IT projects reported to validate existence, cloud relevance, and total project budget. Additionally, we tested completeness of reporting by reviewing all 403 Fiscal Year 2024 IT projects for any unreported cloud projects.	No significant issues.

Source: Office of the Legislative Auditor.

---

[25] *Laws of Minnesota* 2023, chapter 62, art. 6, sec. 12, codified as *Minnesota Statutes* 2025, 16E.03, subd. 5a.

Finding and Recommendation

Cloud Progress Reporting

Minnesota IT Services (MNIT) is required to annually report on the progress of executive branch cloud adoption. These reports must include cloud-related expenditures and current projects that incorporate cloud computing solutions.[26]

In its January 2025 progress report, MNIT reported it had partnered with 390 cloud providers in Fiscal Year 2024, with expenditures totaling over $55 million. We recalculated these expenditures for reporting accuracy and identified some unreported payments.

FINDING

Minnesota IT Services did not include Microsoft Azure support and maintenance costs in its cloud progress reports.

Although MNIT had included support and maintenance costs associated with its Amazon Web Service (AWS) cloud services, MNIT did not include these same types of costs associated with its Microsoft Azure (Azure) cloud services.[27]

Because MNIT codes payments for Azure support within the state's accounting system differently than other cloud expenditures, MNIT erroneously excluded those Azure payments when it extracted data to include within the required progress reports. Including support and maintenance costs in the reports gives a more accurate reflection of the cost to maintain cloud environments. By not including these costs, MNIT understated Azure expenditures by approximately $349,000 for Fiscal Year 2024 and $37,000 for Fiscal Year 2023.[28]

RECOMMENDATION

Minnesota IT Services should include all cloud-related support and maintenance costs in future cloud progress reports.

---

[26] *Laws of Minnesota* 2023, chapter 62, art. 6, sec. 12, codified as *Minnesota Statutes* 2025, 16E.03, subd. 5a.

[27] AWS and Azure provide basic support services with cloud subscriptions. For customers who prefer a higher level of service, these providers offer additional support and maintenance plans, which may include rapid response times for critical issues or added assistance for implementing and troubleshooting cloud solutions.

[28] These amounts represent less than 1 percent of the total cloud expenditures MNIT reported. MNIT told us that it did include appropriate support costs within its January 2026 cloud progress report. OLA did not validate this claim, as the release of the MNIT report was after our audit work had concluded.

OLA

Appendix A – Cloud Terminology

Key Terms Used	Definition
Amazon Web Services (AWS)	Referred to as "AWS" or "AWS Commercial," AWS is a public cloud computing environment that provides multiple IaaS, PaaS and SaaS services, such as computing, analytics, storage, networking, data, application development, identity, and security.
Cloud Computing[a]	Cloud computing is the availability of computing resources (for example, application development tools, data storage, networking capabilities, servers, and software) on demand, over the internet. For many cloud computing services, customers (individual users or tenants) use their internet browser to access computing resources when they are needed, and then release them or shut them down when they are no longer needed. Cloud providers group these pooled resources into appropriate types of services (for example, processing, storage, network) and measure how much a customer uses of the service using metering capabilities.
Cloud Environment	A "cloud environment" refers to a virtual IT environment where cloud computing services operate and includes the hardware, software, networking, and storage resources delivered over the internet or a private network. Applications can be deployed and managed through multiple types of cloud deployment models (such as public and private) and service models (IaaS, PaaS, SaaS), each with different levels of user and service provider responsibilities.[b]
Cloud Deployment Model	A cloud deployment model defines how the cloud infrastructure is organized, where it resides, and who controls it.[c] The National Institute of Standards and Technology (NIST) defines four common cloud deployment models: public cloud, private cloud, community cloud, and hybrid cloud.[d]
Cloud Service Model	A cloud service model refers to the type of computing services delivered in the cloud, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS).[e]
FinOps	FinOps is a cost management methodology for maximizing the value of cloud technologies. It combines financial management principles with cloud engineering and operations to help organizations make informed decisions on how to allocate and manage their cloud costs.[f]
Infrastructure as a Service (IaaS)	This is the most basic category of commercial cloud computing services. IaaS allows customers to rent IT infrastructure, such as servers, virtual machines, storage, networks, and operating systems, from a cloud provider.[g]
Microsoft Azure (Azure)	Referred to as "Azure," "Azure Cloud," or "Azure Commercial," Microsoft Azure is a public cloud computing environment providing multiple IaaS, PaaS, and SaaS services, such as computing, analytics, storage, networking, data, application development, identity, and security.
Pay-As-You-Go	A cloud payment model that allows the customer to pay only for what is used; there are no long-term commitments or upfront costs. For example, if a virtual machine is used for 50 hours, the customer only pays for those 50 hours.
Platform as a Service (PaaS)	This cloud service supplies an on-demand environment for developing, testing, delivering, and managing software applications. PaaS is designed to make it easier for developers to quickly create applications without needing to manage the underlying infrastructure.[h]

Key Terms Used	Definition
Reserved Instances	A cloud payment model that allows the customer to commit to specific cloud resources for one year or three years. In exchange, the cloud service provider offers a discount. For organizations with steady, predictable workloads, reserved instances can offer significant cost savings, compared to pay-as-you-go prices, but requires an upfront one-time payment.
Savings Plans	Like reserved instances, savings plans can be more flexible and are used for more dynamic or unpredictable workloads.
Software as a Service (SaaS)	This cloud service delivers software applications on demand, over the internet, typically on a subscription basis. SaaS service providers host and manage the application software and underlying infrastructure and handle any maintenance, like software upgrades and security patching.[i]
Spot Virtual Machines/Spot Instances	With spot virtual machines, also known as spot instances, customers can provision unused Azure compute capacity at deep discounts of up to 90 percent compared to pay-as-you-go prices. However, at any point in time when Azure needs the capacity back, the Azure infrastructure will evict the user from the spot virtual machines. As such, these are not ideal solutions for all purposes.
Virtual Machines	Virtual machines are one of several types of on-demand, scalable computing resources that Azure offers. Virtual machines (servers and desktop computers) give organizations the flexibility of implementing computing devices without having to buy and maintain the physical hardware.

[a] *Minnesota Statutes* 2025, 16E.03, subd. 1(g), defines cloud computing as the meaning described by the National Institute of Standards and Technology of the U.S. Department of Commerce in Special Publication 800-145 (September 2011). The definition provided here uses common language to paraphrase the technical definition of cloud computing provided by NIST.

[b] Based on Rick Sturm, Carol Pollard, and Julie Craig, "Application Performance Management (APM) in the Digital Enterprise, Chapter 4 – Application Management in the Cloud" (2017), https://www.sciencedirect.com /topics/computer-science/cloud-environment.

[c] Based on Derrick Rountree and Ileana Castrillo, "The Basics of Cloud Computing: Understanding the Fundamentals of Cloud Computing in Theory and Practice" (2014), https://www.sciencedirect.com/topics /computer-science/cloud-deployment-model.

[d] Rountree and Castrillo, "The Basics of Cloud Computing."

[e] National Institute of Standards and Technology, *NIST Special Publication 800-145: The NIST Definition of Cloud Computing* (September 2011).

[f] "What Is FinOps?", FinOps Foundation, accessed April 25, 2025, https://www.finops.org/introduction/what-is -finops/.

[g] "Infrastructure as a Service (IaaS)," U.S. General Services Administration, Cloud Information Center, accessed August 18, 2025, https://cic.gsa.gov/index.php/solutions/iaas.

[h] "Platform as a Service (PaaS)," U.S. General Services Administration, Cloud Information Center, accessed August 18, 2025, https://cic.gsa.gov/solutions/paas.

[i] "Software as a Service (SaaS)," U.S. General Services Administration, Cloud Information Center, accessed August 18, 2025, https://cic.gsa.gov/solutions/saas.

Source: Office of the Legislative Auditor.

Appendix B – MNIT's Cloud History

Year	Key Milestones
2010	Minnesota's executive branch began an initiative to move agencies to Microsoft Office 365 for email and collaboration tools.
2011–2013	MNIT consolidated 49 data centers into 4 and encouraged innovation in cloud services at agencies.
2018–2019	MNIT migrated the Minnesota Department of Health's application portfolio to Amazon Web Services (AWS)-based infrastructure.
2020	MNIT partnered with the Department of Labor and Industry to launch Work Comp Campus, a new Azure portal for filing and accessing workers' compensation claims.
2020–2021	MNIT issued an RFP to identify a primary cloud provider for infrastructure services. Microsoft Azure was awarded the contract in early 2021.[a]
2023	The Legislature appropriated $33.6 million over four years to support the executive branch's cloud transformation.[b]
2024	Ongoing migration to the cloud increased with over 1,500 servers migrated, 31 agencies engaged in migration activities, and 250 applications migrated.[c]

[a] MNIT issued the RFP in December 2020, awarded the contract to Microsoft Azure, and signed the contract on April 30, 2021.

[b] *Laws of Minnesota* 2023, chapter 62, art. 1, sec. 10.

[c] Minnesota IT Services, *2024 MNIT Annual Report: Digital Leadership in a Changing World,* https://mn.gov/mnit/assets/MNIT-Annual-Report-2024_tcm38-665874.pdf, 15, accessed January 21, 2025.

Source: Office of the Legislative Auditor.

OLA

Appendix C – Compliance Requirements Tested

Area Tested	Criteria

Cloud Procurement
• Procurement Policies and Procedures
• Request for Proposals (RFP) Development
• RFP Evaluation and Award
• RFP Negotiation
• Cloud Services Contracts
• Risk Authorization and Management Program (RAMP)
	• Minnesota Department of Administration, Office of State Procurement:
	   ○ Purchasing Policy 10, *Status of Information in Bids and Proposals Submitted to the State of Minnesota*, revised April 2017
	   ○ Purchasing Policy 14, *Instructions for Reporting Purchasing Violations, Vendor Protests, and Mis-awards*, revised April 2017
	   ○ Purchasing Policy 17, *Requirements for Signing Documents and Cancelling Contracts*, revised April 2017
	   ○ Purchasing Policy 23, *Acquisitions ALP Policy, Procedure, and Training Overview*, revised July 2023
	   ○ Purchasing Policy 24, *MNIT Services Authority for IT Purchases and Contracts*, revised September 2024
	   ○ Purchasing Policy 25, *Amending Contracts*, revised April 2017
	   ○ Purchasing Policy 35, *Revised Instructions for Applying Preferences*, revised July 2023
	• National Association of State Procurement Officials (NASPO), "*Procurement Toolbox Issue 6: The Value of Negotiations*," https://cdn.naspo.org/RI/ProcurementToolboxIssue6_TheValueofNegotiations.pdf, accessed June 3, 2025
	• Center for Digital Government, *Best Practice Guide for Cloud and As-A-Service Procurements*, Version 2 (2022)
	• "About FedRAMP Marketplace: Marketplace Designations," U.S. General Services Administration, FedRAMP Project Management Office, accessed August 15, 2025, https://www.fedramp.gov/about-marketplace/
	• Industry recommendations from advisory firms specializing in enterprise software licensing and cloud contract negotiations[a]

Cloud Asset Inventory • Inventory Policies and Procedures • Inventory Accuracy • Inventory Completeness • Inventory Consistency	• Minnesota IT Services, *Secure Configuration Standard: Control 3, System Inventory, Version 1.8*, issued January 2016, revised December 2024; *Azure Resource Naming Standard, Version 1.0* (December 2021); and *Azure Resource Tagging Configuration Standard Version 1.0* (December 2021) • National Institute of Standards and Technology, *NIST Special Publication 800-53, Rev. 5.1.1, Security and Privacy Controls for Information Systems and Organizations: Control CM-8, System Component Inventory* (November 2023) • Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing v5, Section 2.3.2: Cloud Registry* (February 2025)

Area Tested	Criteria
Cloud Cost and Usage Data, Monitoring, and Anomaly Detection • Policies and Procedures • Pricing Data Accuracy • Cost and Usage Data Accuracy • Cost Monitoring and Anomaly Detection	• Minnesota Management and Budget, Statewide Operating Policy 0802-01, *Payment Request, Preparation, and Approval*, issued July 2011, revised July 2022 • Minnesota Department of Administration, Office of State Procurement, *Contract Release C-1121(5): Computer: Cloud Solutions, Web-Based Software, and Related Services* (January 10, 2025) • Minnesota Department of Administration, Office of State Procurement, *AWS Cloud Hosting Services Contract, SWIFT Contract Numbers 128953, T-Number C-1121(5)* (July 26, 2017) • Minnesota Department of Administration, Office of State Procurement, *Microsoft Cloud Hosting Azure Enrollment* (April 30, 2021) • "Azure Cost Management: Ingest Cost Details Data Overview," Microsoft, accessed March 19, 2025, https://learn.microsoft.com/en-us/azure/cost-management-billing/automate/automation-ingest-usage-details-overview#pricing-behavior-in-cost-and-usage-details • "AWS Data Exports User Guide: Focus 1.0 with AWS columns," Amazon Web Services, accessed May 14, 2025, https://docs.aws.amazon.com/cur/latest/userguide/what-is-data-exports.html • "FinOps Framework: Reporting & Analytics," FinOps Foundation, accessed August 8, 2025, https://www.finops.org/framework/capabilities/reporting-analytics/ • "FinOps Framework: Anomaly Management," FinOps Foundation, accessed August 8, 2025, https://www.finops.org/framework/capabilities/anomaly-management/
Cloud Expenditures • Policies and Procedures • Approval • Prompt Payment • Reconciliation • Expense Reporting • Data Accuracy • Use of Appropriation	• *Minnesota Statutes* 2025, 16A.065 • *Minnesota Statutes* 2025, 16A.15 • *Minnesota Statutes* 2025, 16A.124 • Minnesota Management and Budget: ◦ Statewide Operating Policy 0801-01, *Prompt Payment Processing*, issued December 2015 ◦ Statewide Operating Policy 0802-01, *Payment Request, Preparation*, *and Approval*, issued July 2011, revised July 2022 ◦ Statewide Operating Policy 0802-04, *Matching Rules and Requirements*, issued June 2015 • Minnesota IT Services, Accounts Payable Policies and Procedures: ◦ Invoice Approval Policy ◦ Invoice Payment Process Guidance ◦ IT Receipt Form ◦ Electronic Documentation Policy • *Laws of Minnesota* 2023, chapter 62, art. 1, sec. 10(c)
Cloud Progress Reporting • Cloud Reporting Submissions • Cloud-Related Expenditures • Cloud Projects	• *Minnesota Statutes* 2025, 16E.03, subd. 5a

[a] We used publicly available data from two leading independent advisory firms specializing in enterprise software licensing and cloud contract negotiations: Directions on Microsoft located in Kirkland, WA, and Redress Compliance located in Fort Lauderdale, FL.

Source: Office of the Legislative Auditor.

Minnesota IT Services
600 N. Robert St.
Suite 2800
St. Paul, MN 55146

March 20, 2026

Judy Randall, Legislative Auditor
Office of the Legislative Auditor
Room 140 Centennial Office Building
658 Cedar Street
St. Paul, MN 55155

Dear Legislative Auditor Randall,

Thank you for the opportunity to respond to the Cloud-Based Information Technology Services audit report. We appreciate the Office of the Legislative Auditor's work assessing the effectiveness of state programs and providing feedback that helps improve the efficiency, compliance, and performance of the services we deliver for Minnesotans.

MNIT values that this audit provides legislators and the public with a broad view of our efforts to improve technology infrastructure and platform service delivery through an intentional cloud strategy. As the report notes, this approach is achieving cost efficiencies for agency partners and taxpayers while also strengthening resiliency, recovery capabilities, and access to modern, market-leading functionality for state services.

Below, please find MNIT's perspective regarding the report's finding and recommendation.

Report Finding:

Minnesota IT Services did not include Microsoft Azure support and maintenance costs in its cloud progress reports.

Report Recommendation:

Minnesota IT Services should include all cloud-related support and maintenance costs in future cloud progress reports.

MNIT Response:

The 2026 Cloud Progress Report incorporated maintenance and support cost information following updates to MNIT's accounting practices. Prior to these changes, MNIT paid for broad coverage of support and maintenance of many Microsoft products through a unified support model, including the Azure product line. As a result of discussions during the course of this audit, MNIT updated its cost-tracking procedures to extract the costs for Azure support and maintenance and provide a clearer basis of cost comparison in the cloud vendor space. This finding is fully resolved, and future reports will include the enhanced cost tracking measures recommended by the OLA.

Thank you again for the opportunity to participate in this audit and for your continued partnership in strengthening MNIT's services and programs.

Sincerely,

Jon Eichten
Commissioner and State Chief Information Officer

OLA

OLA

Financial Audit Staff

Judy Randall, *Legislative Auditor*
Lori Leysen, CPA, *Deputy Legislative Auditor*

Audit Directors
Ryan Baker, CPA, CFE
Jordan Bjonfald, CPA
Kayla Borneman, CPA
Mark Mathison, CISA, CISSP, CPA (inactive)
Heather Rodriguez
Joe Sass, CISA
Valentina Stone, CPA
Scott Tjomsland, CPA
Zach Yzermans, CPA

Audit Team Leads
Shannon Hatch, CFE
Gabrielle Johnson, CPA
Holly Runia

Senior Auditors
Joseph Anderson
Ria Bawek
Tyler Billig, CPA
Nicholai Broekemeier
Ryan Fetterer
Deb Frost, CISA
Dustin Juell, CompTIA Security+
Christian Knox
Lisa Makinen, CPA
Alec Mickelson
Erick Olsen
Rob Riggins, CISA, CISSP
Zakeeyah Taddese
Emily Wiant

Auditors
TJ Davies
Gabrielle Gruber
Dylan Harris
Nicole Heggem
Benjamin Path
Cary Sumague
Robert Schmitz
Niari Woods
Peng Xiong

OLA | OFFICE OF THE
LEGISLATIVE AUDITOR

Office of the Legislative Auditor
Suite 140
658 Cedar Street
Saint Paul, MN 55155