Memorandum from the Office of the Inspector General

June 17, 2025

Tammy W. Wilson

REQUEST FOR MANAGEMENT DECISION – AUDIT 2024-17521 – CLOUD INVENTORY

Due to the Tennessee Valley Authority's (TVA) increased use of cloud services, we conducted an audit of TVA's cloud inventory. Cloud services include products such as infrastructure, applications, development tools, and data storage that are offered by third-party providers and accessed over the internet. Cloud services allow users to access resources, without managing physical servers themselves or running software applications on their own machines. Our objective was to determine if TVA maintained an accurate and complete cloud inventory.

Although we determined TVA's (1) defined processes related to managing cloud inventory were designed in alignment with identified best practices, and (2) access controls for the cloud inventory were operating effectively, TVA does not maintain an accurate and complete cloud inventory. Specifically, (1) cloud services procured outside of the information technology (IT) organization's procurement process were not included in inventory, (2) reconciliation controls did not include all available sources to identify cloud services, and (3) required fields in existing inventory data were incomplete.

We made four recommendations to TVA management to improve the accuracy and completeness of the cloud inventory.

TVA management agreed with our recommendations. See the Appendix for TVA management's complete response.

<u>BACKGROUND</u>

TVA began a digital transformation process in 2020 and adopted a technology modernization strategy with a focus on asset management and cloud adoption in 2024. Cloud services include products such as infrastructure, applications, development tools, and data storage that are offered by third-party providers and accessed over the internet. Cloud services allow users to access resources, without managing physical servers themselves or running software applications on their own machines. These services are sorted into several different categories, or service models, including Software-as-a-Service, Platform-as-a-Service, and Infrastructure-as-a-Service.

According to TVA Standard Programs and Processes (SPP) 12.405, *IT Asset Procurement and Management*, all software assets, whether purchased, developed, or supported by TVA IT, shall be entered and maintained in the IT asset management system. In addition, no software of any type may be purchased using any means other than IT's procurement process. This restriction also applies to cloud services.

We identified best practices for managing cloud inventory from the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS).[1] NIST 800-53[2] requires agencies to document an inventory of system components that (1) accurately reflects the system and all components within the system, (2) does not include duplicate accounting of components or components assigned to any other system, and (3) is at the level of granularity deemed necessary for tracking and reporting. CIS maintains a listing of critical security controls, which includes *Inventory and Control of Software Assets*. This control states the organization should "actively manage (inventory, track, and correct) all software (operating system and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution."[3]

CIS states, "it is imperative to maintain a comprehensive list of cloud software assets to identify and mitigate any vulnerabilities and data associated with the software" being managed.[4] The cloud inventory should be used to ensure the risks associated with cloud services are properly understood and mitigated when warranted. Due to TVA's increased use of cloud services, we performed an audit of TVA's cloud inventory.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine if TVA maintained an accurate and complete cloud inventory. The scope of this audit was cloud services in use in the TVA environment. To achieve our objective, we:

- Identified and reviewed relevant TVA agency-wide policies, procedures, and technical standards to gain an understanding of the current state of cloud procurement and inventory processes, including TVA-SPP-12.405, *IT Asset Procurement & Management.*
- Inquired of TVA IT, Supply Chain, and Financial Shared Services personnel to gain an understanding and current state of cloud procurement and inventory processes.
- Performed a gap analysis of TVA's policies with applicable NIST and CIS best practices to identify any gaps.
- Identified internal control significant to the audit and performed testing to the extent necessary to address the audit objective. Specifically, we:
  - Obtained an understanding of the controls and identified required fields and reconciliation as key internal controls.

[1] Center for Internet Security, a nonprofit organization, is a collaboration of experts in the field of IT security.

[2] NIST Special Publication 800-53 (Revision 5), *Security and Privacy for Information System and Organizations, September 2020,* <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>*,* accessed on October 16, 2024.

[3] CIS Critical Security Controls® Version 8, <http://www.cisecurity.org/controls/>, CIS Control 2, accessed on October 17, 2024.

[4] CIS Controls Cloud Companion Guide Version 8, <https://www.cisecurity.org/> accessed on April 22, 2025.

  - Assessed the design of key internal controls by reviewing applicable policies, procedures, technical standards, and identified best practices to determine if the controls, as designed, were capable of meeting their intended objectives.
  - Assessed implementation and operating effectiveness of key internal controls.
  - Assessed the design, implementation, and operating effectiveness of internal controls to prevent duplicates and restrict unauthorized access.
- Obtained TVA's cloud inventory records as of February 24, 2025, to determine if required fields contained necessary information to maintain an accurate inventory.
- Identified and reviewed other data sources to determine if cloud assets regardless of procurement method were included in TVA's cloud inventory.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require 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 objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

FINDINGS

Although we determined TVA's (1) defined processes related to managing cloud inventory were designed in alignment with identified best practices, and (2) access controls for the cloud inventory were operating effectively, TVA does not maintain an accurate and complete cloud inventory. Specifically, (1) cloud services procured outside of the IT organization's procurement process were not included in inventory, (2) reconciliation controls did not include all available sources to identify cloud services and (3) required fields in existing inventory data were incomplete.

CLOUD SERVICES PROCURED OUTSIDE OF IT DEFINED PROCESS WERE NOT INCLUDED IN INVENTORY

According to TVA-SPP-12.405, *IT Asset Procurement & Management,* all software assets, whether purchased, developed, or supported by TVA IT, shall be entered and maintained in the IT asset management system. In addition, no software of any type may be purchased using any means other than the IT procurement process. This restriction also applies to cloud services. However, we identified cloud services that were purchased using (1) TVA credit cards and (2) purchase orders that were not included in the cloud inventory. Also, through interviews with TVA personnel, we identified other cloud services being (1) tracked for licensing and subscription cost purposes and (2) accessed by TVA assets that were not included in the cloud inventory. Therefore, we determined there were no controls preventing or detecting cloud services procured outside of the IT procurement process, resulting in an incomplete inventory.

A recent Office of the Inspector General audit of TVA's credit card purchases identified seven purchases of IT-related assets that should have been purchased through the IT procurement process.[5] Three of these seven IT-related purchases were for cloud

[5] Audit No. 2024-17501, *TVA One Card*, March 17, 2025.

services. One of three were included and the remaining two were not included in TVA's cloud inventory.

Controls to prevent cloud service procurement and detect cloud services procured outside of the IT procurement process will allow TVA to maintain a more complete cloud inventory regardless of procurement method.

RECONCILIATION CONTROLS DID NOT INCLUDE AVAILABLE SOURCES TO IDENTIFY CLOUD SERVICES

TVA-SPP-12.405, *IT Asset Procurement & Management*, states review of assets listed in the IT asset management system may occur annually, or more often as deemed necessary, and may be reconciled with other data sources or tools used within IT.

While TVA is reconciling the IT asset management system to some data sources or tools, we identified additional data sources or tools used within IT that TVA is not reconciling to the cloud inventory. Specifically, cloud services being (1) tracked for licensing and subscription cost purposes and (2) accessed by TVA assets were not included in reconciliations conducted by TVA. In addition, we identified data sources outside of IT that could be reconciled, such as cloud services purchased using TVA credit cards and purchase orders, to identify potential new cloud services.

As previously mentioned, we found cloud services procured outside of IT's defined process were not included in inventory from additional data sources or tools. Strengthened reconciliation controls will allow TVA to identify new cloud services that have been added and ensure the completeness of data.

CLOUD INVENTORY MISSING DATA IN REQUIRED FIELDS

We reviewed the cloud inventory as of February 24, 2025, to determine if required fields contained necessary information to maintain an accurate inventory. These fields, required by TVA, include information such as architecture type, business owner, supported contact, and change group. We identified five blanks in four required fields, impacting four different cloud services. According to TVA management, they were aware of the missing data and were in the process of addressing the issue. Missing data in required fields results in inaccurate inventory records.

RECOMMENDATIONS

We recommend the Vice President, Chief Information and Digital Officer, IT:

1. Implement controls to prevent and detect disallowed cloud services procured outside of the IT procurement process, in conjunction with TVA Supply Chain and TVA Financial Services personnel.

2. Update the cloud inventory reconciliation process to include other data sources of cloud services procured or in use to improve cloud inventory completeness.

3. Review and update the cloud inventory as appropriate.

4. Implement a periodic process to identify and update blank required fields to improve cloud inventory accuracy.

TVA Management's Comments – In response to our draft audit report, TVA management agreed with our recommendations. See the Appendix for TVA management's complete response.

- - - - - -

This report is for your review and information. Please advise us of your management decision within 60 days from the date of this report. In accordance with the Inspector General Act of 1978, as amended, the Office of the Inspector General is required to report to Congress semiannually regarding audits that remain unresolved after 6 months from the date of report issuance.

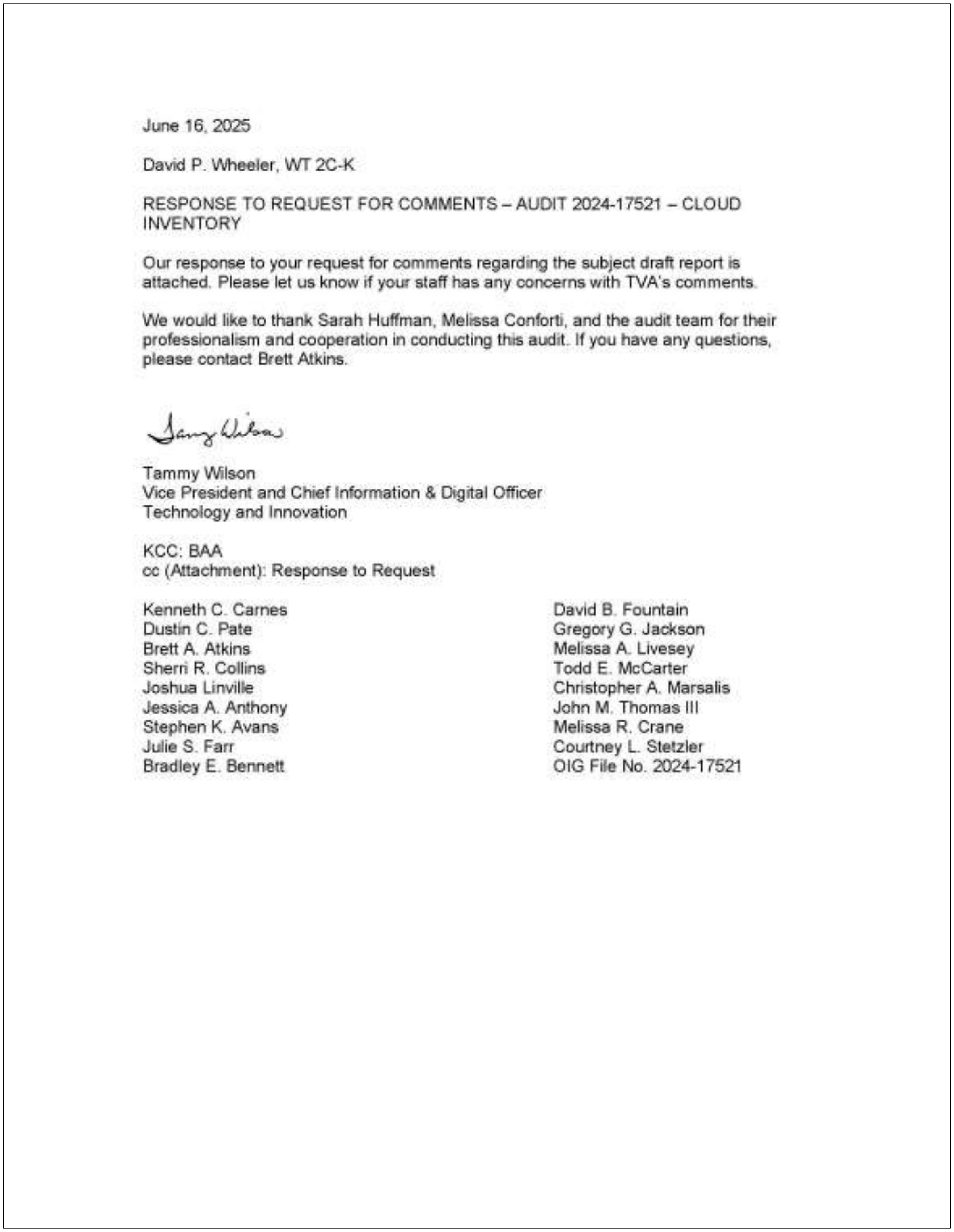
If you have any questions, please contact Sarah E. Huffman, Director, Information Technology Audits, at (865) 633-7345. We appreciate the courtesy and cooperation received from your staff during the audit.

David P. Wheeler

David P. Wheeler
Assistant Inspector General
(Audits and Evaluations)

MLC:KDS
cc: TVA Board of Directors
Brett A. Atkins
Tammy C. Bramlett
Laura J. Campbell
Kenneth C. Carnes
Sherri R. Collins
Melissa R. Crane
Jessica Dufner
Melissa A. Livesey
Jill M. Matthews
Todd E. McCarter
Jeannette Mills
Don A. Moul
Dustin C. Pate
Thomas C. Rice
Ronald R. Sanders II
Courtney L. Stetzler
Josh Thomas
Rebecca C. Tolene
Ben R. Wagner
Diane T. Wear
OIG File No. 2024-17521

APPENDIX
Page 1 of 2



June 16, 2025

David P. Wheeler, WT 2C-K

RESPONSE TO REQUEST FOR COMMENTS – AUDIT 2024-17521 – CLOUD INVENTORY

Our response to your request for comments regarding the subject draft report is attached. Please let us know if your staff has any concerns with TVA's comments.

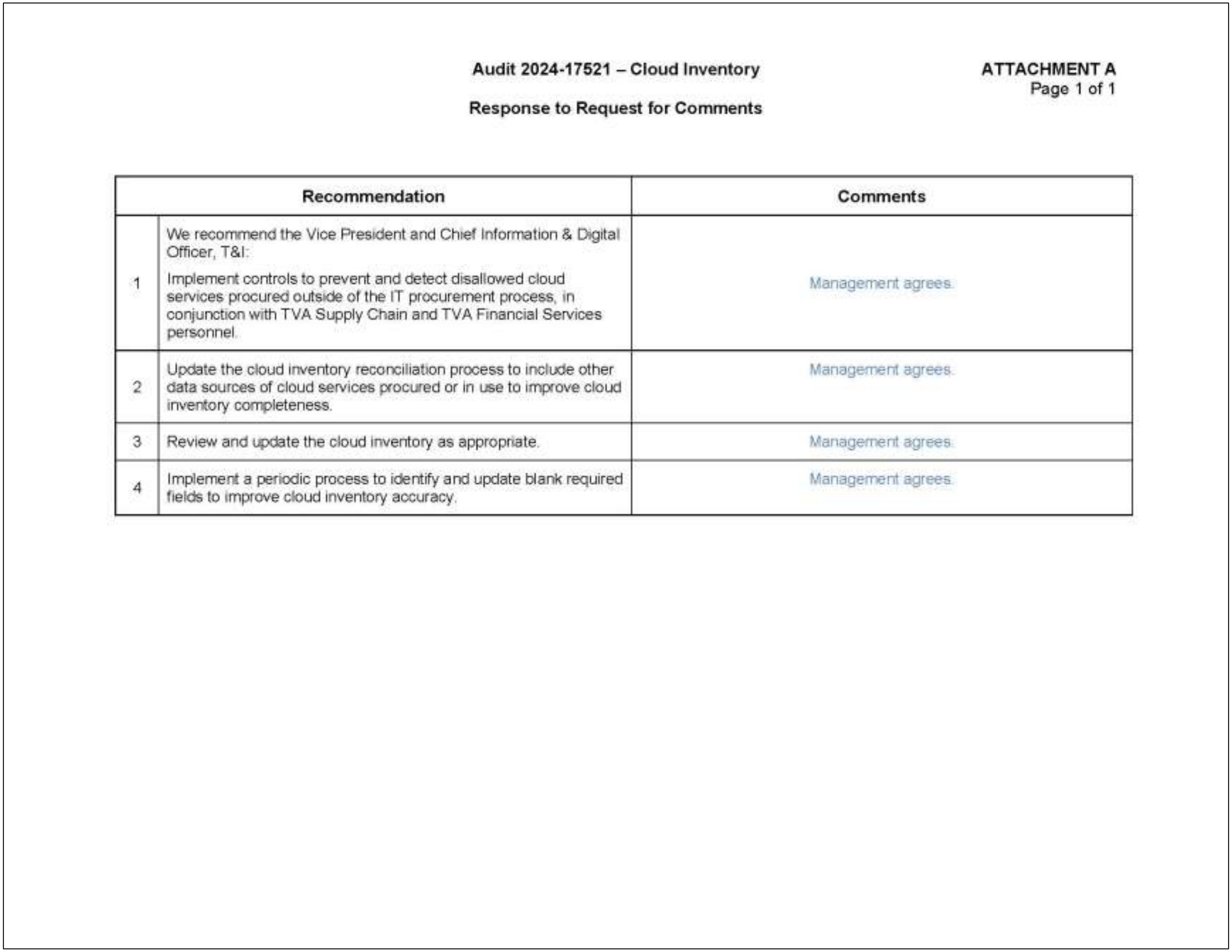
We would like to thank Sarah Huffman, Melissa Conforti, and the audit team for their professionalism and cooperation in conducting this audit. If you have any questions, please contact Brett Atkins.

Tammy Wilson
Vice President and Chief Information & Digital Officer
Technology and Innovation

KCC: BAA
cc (Attachment): Response to Request

Kenneth C. Carnes
Dustin C. Pate
Brett A. Atkins
Sherri R. Collins
Joshua Linville
Jessica A. Anthony
Stephen K. Avans
Julie S. Farr
Bradley E. Bennett

David B. Fountain
Gregory G. Jackson
Melissa A. Livesey
Todd E. McCarter
Christopher A. Marsalis
John M. Thomas III
Melissa R. Crane
Courtney L. Stetzler
OIG File No. 2024-17521



Audit 2024-17521 – Cloud Inventory

ATTACHMENT A
Page 1 of 1

Response to Request for Comments

Recommendation		Comments
1	We recommend the Vice President and Chief Information & Digital Officer, T&I: Implement controls to prevent and detect disallowed cloud services procured outside of the IT procurement process, in conjunction with TVA Supply Chain and TVA Financial Services personnel.	Management agrees.
2	Update the cloud inventory reconciliation process to include other data sources of cloud services procured or in use to improve cloud inventory completeness.	Management agrees.
3	Review and update the cloud inventory as appropriate.	Management agrees.
4	Implement a periodic process to identify and update blank required fields to improve cloud inventory accuracy.	Management agrees.