Internal Audit Report

Application Security & Access Management focusing on AASHTOWare

Todd Wilkins, CISA, CRISC, CISM, CDPSE

2026

SOUTH CAROLINA OFFICE OF THE STATE AUDITOR

1. Executive Summary

Objective

Management's objective with AASHTOWare application security and access control is to ensure the effective and efficient safeguarding of transportation data and related business processes to minimize operational, compliance, and security risks while supporting organizational goals and objectives. Effective access management is critical to prevent unauthorized use or modification of data, preserve system integrity, and ensure that AASHTOWare continues to support agency operations in a secure and reliable manner. The goal of the process is to maintain confidence that the system is properly protected, that users have only the access they need to perform their duties, and that the application continues to align with the agency's mission and regulatory requirements. See Appendix A for process descriptions.

Internal Audit Services' objective is to provide assurance over the design and operation of application security and access control for AASHTOWare. Specifically, we evaluated whether current practices align with the requirements of the statewide DIS-200 v1 standard, which is mandatory for state agency compliance. While this engagement references DIS-200 v1 as the benchmark, management should consider addressing any corrective actions in alignment with DIS-200 v2, which maps to NIST Cybersecurity Framework (CSF) v2 subcategories and NIST 800-53r5 controls. Our goal is to provide assurance that AASHTOWare is appropriately managed, adequately protected, and continues to align with business needs, while minimizing risks of unauthorized access, data loss, or operational disruption.

The objectives of this audit are to:

- Evaluate whether user access to AASHTOWare is appropriately granted, modified, and removed in a timely manner.
- Assess enforcement of least privilege and segregation of duties within AASHTOWare roles and permissions.
- Confirm monitoring, logging, and review processes are in place to detect inappropriate or unauthorized activity.
- Validate that periodic user access reviews are conducted and documented in alignment with DIS-200 requirements.
- Compare observed practices to statewide DIS-200 v1 controls and highlight opportunities for future alignment with DIS-200 v2.

Background

As part of the Internal Audit Plan, Internal Audit Services is conducting an evaluation of application security and access control practices for the agency's AASHTOWare suite. AASHTOWare is a mission-critical suite of applications that supports the agency's transportation operations, including project management, construction, and related business functions. Given its role in managing operational data and facilitating statewide transportation

activities, securing AASHTOWare and ensuring appropriate access is a foundational element of the agency's IT governance responsibilities.

This audit aligns with the State's Information Security (Infosec) Program, which requires agencies to implement security practices that safeguard information systems across technical, physical, and personnel domains. The Infosec Program is codified through the DIS-200 policy standard and related guidance, which establishes statewide benchmarks for control design and operation. Evaluating AASHTOWare's security and access practices against these standards helps the agency assess its current posture and identify opportunities to strengthen protections over critical systems and data.

Early in 2025, the Department of Administration conducted an external audit that included a limited review of application security and access controls for five applications, two of which were part of the AASHTOWare suite. Building on that foundation, Internal Audit Services has extended the scope to include the remaining AASHTOWare modules not previously reviewed. This included application modules that are used within Bridge Management and the Materials & Research Office. This approach provides management with a more comprehensive assessment of security and access practices across the entire suite, ensuring that risks are consistently identified and addressed.

Conclusion

Observations, recommendations, and management action plans are developed and discussed with SCDOT Executive Leaders. This information is not included in this report due to the confidential nature of information security and is closed to public release by SC Code of Laws Section 30-4-20 (c).

Contents

1. Executive Summary 1
   - Objective 1
   - Background 1
   - Conclusion 2
2. Forward 4
   - Authorization 4
   - Statement of Independence 4
   - Report Distribution 4
   - Acknowledgement 4
   - Lead Auditor 4
   - Reviewer 4
3. Internal Auditor's Report 5
4. Engagement Overview 6
   - Background 6
   - Objective 7
   - Scope 8
   - Methodology 9
5. Conclusion 10
   - Asset Lifecycle Management Controls 10
   - Observations and Recommendations 11
   - Development of Management Action Plans 11
   - Reporting of Confidential Information 11
   - Appendix A - Process Descriptions 12
   - Process Overview 12
   - Appendix B – Generic Maturity Model 13

2. Forward

Authorization

The South Carolina Office of the State Auditor established the Internal Audit Services division (IAS) pursuant to SC Code Section 57-1-360 as revised by Act 275 of the 2016 legislative session. IAS is an independent, objective assurance and consulting function designed to add value and improve the operations of the South Carolina Department of Transportation (SCDOT). IAS helps SCDOT to achieve its objectives by bringing a systematic, disciplined approach to evaluating the effectiveness of risk management, internal control, and governance processes and by advising on best practices.

Statement of Independence

To ensure independence, IAS reports administratively and functionally to the State Auditor while working collaboratively with SCDOT leadership in developing an audit plan that appropriately aligns with SCDOT's mission and business objectives and reflects business risks and other priorities.

Report Distribution

This report is intended for the information and use of the SCDOT Commission, SCDOT leadership, the Chairman of the Senate Transportation Committee, the Chairman of the Senate Finance Committee, the Chairman of the House of Representatives Education and Public Works Committee, and the Chairman of the House of Representatives Ways and Means Committee. However, this report is a matter of public record and its distribution is not limited.

Acknowledgement

We wish to thank members of management and staff in the Engineering, Finance and Administration, and Information Technology for their cooperation in assessing risks and developing actions to improve internal controls and enhance operating performance.

Lead Auditor

Todd Wilkins, CISA, CRISC, CISM, CDPSE
Associate Director

Reviewer

Mark LaBruyere, CPA, CIA
Director of Internal Audit Services

SOUTH CAROLINA OFFICE OF THE STATE AUDITOR
1401 Main Street, Suite 1200 • Columbia, SC 29201

3. Internal Auditor's Report

5/15/2026

Mr. Justin P. Powell, Secretary of Transportation
and
Members of the Commission
South Carolina Department of Transportation
Columbia, South Carolina

We have completed an evaluation of application security and access management practices for the agency's AASHTOWare suite. The objective of this engagement was to support management in strengthening security and governance by evaluating the relative risk of AASHTOWare modules and assessing selected controls designed to manage those risks.

Our engagement included two aspects:

- A riskiness evaluation to identify and prioritize AASHTOWare modules for further review, and
- An assessment of application security and access management practices within the selected modules to determine alignment with state information security requirements.

We planned and performed the engagement with due professional care to obtain sufficient, appropriate evidence to provide a reasonable basis for our observations and recommendations. Our observations, recommendations, and management's action plans were discussed with management.

Mark A. LaBruyere
Director of Internal Audit Services

4. Engagement Overview

Background

The South Carolina Department of Transportation (SCDOT) recognizes the critical role that secure application access plays in protecting operations, sensitive data, and public trust. Application Security and Access Management is a foundational component of cybersecurity, ensuring that only authorized users can access the right systems, at the right time, for the right purpose. Weaknesses in this area can expose the organization to risks such as unauthorized activity, data breaches, compliance failures, and operational disruptions.

The AASHTOWare suite is central to the agency's mission and provides tools for project planning, construction management, bridge design and rating, bridge management, pavement analysis, and safety oversight. The agency has implemented five of the six available modules, with deployment models spanning both on-premises and cloud environments. Some modules are fully operational, while others were only recently acquired and are not yet in production. Collectively, these systems support engineering, decision-making, and compliance across the agency's core functions.

Early 2025, the Department of Administration conducted an information security audit under the DIS-200 framework, which included AASHTOWare Project but excluded the other modules. Given the importance of the AASHTOWare suite to agency operations, Internal Audit Services (IAS) recommended extending the review to include the remaining modules. This decision was based on both risk reduction and compliance assurance needs, ensuring that all modules receive appropriate oversight and alignment with state information security requirements.

To scope this engagement, IAS employed a riskiness questionnaire to evaluate each AASHTOWare module across dimensions such as mission impact, data sensitivity, system integration, user community, external access, and recent audit history. This targeted approach allowed IAS to prioritize modules for review while minimizing burden on system owners. Instead, IAS leveraged prior planning work from the Department of Administration and tailored its efforts to focus on specific areas of application security and access control.

This audit aligns with the State's Information Security Program, anchored in the DIS-200 standard. In this engagement, IAS evaluated approximately 30 controls across six key principles of application security and access management:

1. **Identification & Accountability** – Every user and system must be uniquely recognized and held responsible for their actions. This ensures confidence in system activity, supports regulatory compliance, and provides clear traceability when issues arise.

2. **Least Privilege & Controlled Access** – Access is granted on a "need-to-know" basis. Users receive only the access necessary to perform their role, with stronger safeguards for sensitive or high-risk areas. This minimizes misuse, error, and exposure of sensitive data.

3. **Authentication Strength & Password Management** – Strong authentication underpins digital trust. Effective credential management prevents compromise,

protects sensitive accounts, and ensures that outdated or weak practices do not undermine security.

4. **Session & Account Security** – Sessions and accounts are actively protected. Idle sessions are terminated, repeated failed logins are blocked, and users are reminded of expectations through banners and notices. These measures reduce the attack surface and strengthen user accountability.

5. **Monitoring, Logging & Auditability** – System activity must be transparent and verifiable. Effective monitoring and audit logs provide visibility into security events, support rapid incident response, and ensure compliance. This accountability builds organizational trust and resilience.

6. **System Integrity & Baseline Protection** – Systems must remain secure, consistent, and resilient. By hardening configurations, protecting backups, and maintaining approved baselines, the organization ensures operational stability, rapid recovery, and continued confidence in IT operations.

The audit is not intended to provide a punch-list of discrete control gaps. Instead, it emphasizes how well the agency's access management practices support maturity, accountability, and resilience. By grounding this review in principles rather than individual control deficiencies, IAS seeks to provide management with insights that strengthen processes over the long term and ensure that AASHTOWare is managed in a secure, compliant, and mission-aligned manner.

Objective

Management's objective for AASHTOWare's application security & access control is to ensure that system access and identity management practices safeguard agency resources, maintain compliance with statewide security standards, and support the integrity and reliability of operations. Access to AASHTOWare must be provisioned and monitored in a way that reduces the risk of unauthorized use, ensures accountability, and enables system owners to meet both business and regulatory expectations.

IAS, in collaboration with IT Services, was asked to:

1. Evaluate compliance with DIS200 requirements and determine whether access control and identity management practices within AASHTOWare are consistent with statewide security standards.

2. Identify gaps and opportunities where controls may be incomplete, inconsistent, or capable of refinement to improve security, operational efficiency, and user accountability.

3. Validate role-based access and segregation of duties to confirm that user accounts, roles, and group memberships are appropriately defined, provisioned, and monitored to reduce the likelihood of unauthorized access or conflicts of interest.

4. Provide risk-informed insights to help management prioritize corrective actions and strengthen practices based on potential business impact.

5. Encourage standardization and awareness by using the audit as a tool to promote consistent, repeatable processes across all AASHTOWare applications, ensuring system owners and custodians have clear expectations for secure operations.

Internal Audit Services' objective is to provide assurance on the extent to which internal controls and supporting processes for AASHTOWare are designed and operating effectively to manage risks related to access, identity, and accountability. This includes assessing how well practices align with statewide security requirements, support operational effectiveness, and contribute to the agency's overall IT security posture.

Scope

The scope of this audit included a focused evaluation of the agency's implementation and management of the AASHTOWare suite of applications, excluding the AASHTOWare applications that were previously audited early 2025 by Department of Administration. This included application modules that are used within Bridge Management and the Materials & Research Office. The review emphasized whether user access and identity management practices for these applications are designed and operating effectively to safeguard data, enforce accountability, and support compliance with mandatory state security requirements (DIS-200 v1).

The audit addressed the following areas:

- **User Access Management**: Assessed the processes for user provisioning, de-provisioning, and periodic review to ensure that access is appropriate, timely, and properly documented.
- **Role-Based Access Controls**: Evaluated the design and enforcement of role definitions to confirm alignment with job responsibilities and segregation of duties principles.
- **Authentication and Authorization**: Reviewed authentication mechanisms and authorization practices for adequacy, consistency, and adherence to DIS-200 requirements.
- **Monitoring and Logging**: Examined whether access-related activities are logged, monitored, and retained to enable detection of unauthorized activity and support incident response.
- **Backup Processes (High-level & Limited Review)**: Considered whether critical backup procedures supporting AASHTOWare modules are in place and consistent with agency responsibilities.

Control selection for this engagement was based exclusively on the State's DIS-200 v1 security standard, with emphasis on control families directly relevant to AASHTOWare applications (e.g., Access Control, Audit and Accountability, System and Communications Protection, and System and Information Integrity). While certain DIS-200 requirements may conceptually align with broader frameworks such as NIST 800-53, the audit did not adopt external frameworks as a basis for compliance.

The audit approach included planning discussions with system and business owners, walkthroughs of access control processes, evaluation of relevant documentation, and targeted testing of selected controls to validate operating effectiveness.

Out of Scope
The audit did not include the following items:

- A review of source code, operating systems, or underlying infrastructure was not performed.
- Vendor-managed security responsibilities were not assessed beyond the agency's direct obligations.
- Modules not yet in production were excluded to avoid interfering with Go-Live timelines.
- Controls unrelated to AASHTOWare applications, such as enterprise-wide IAM processes or physical access controls, were not included in this review.

Methodology

For the processes included in the engagement scope, we performed the following procedures:

1. **Riskiness Evaluation and Scope Determination:**
   We conducted a riskiness evaluation to help determine which AASHTOWare modules to include in the audit. The evaluation considered factors such as mission impact, data sensitivity, user community, external access, system integrations, update frequency, management reliance, process dependence, existing system documentation, third-party dependencies, and recent audits.
2. **Questionnaire-Based Environment Discovery:**
   System owners and custodians completed structured questionnaires designed to document system environments, account types, roles, authentication practices, and other access management processes. These questionnaires provided insight into the control environment and operational practices.
3. **Interviews and Clarification of Controls:**
   We conducted interviews with key personnel to validate the information from questionnaires, clarify control responsibilities, and understand how access controls are implemented and monitored in practice.
4. **Control Review and Verification:**
   Using the control set established in the prior Department of Administration audit, we verified the existence and design of controls across all in-scope AASHTOWare modules. Testing focused on inquiry, observation, and inspection of supporting evidence, such as screenshots, system logs, and documented procedures.
5. **Principle-Based Evaluation:**
   We evaluated controls and processes in the spirit of maturity, using six key principles. This helped frame our observations in the context of process effectiveness and

strategic alignment. See Appendix B for Generic Maturity Model used by IAS to perform the assessment.

6. **Observation Development and Action Planning:**
   Where gaps or improvement opportunities were identified, observations were developed and discussed with IT and system owners. Action plans were collaboratively reviewed to support remediation, compliance with DIS-200 requirements, and alignment with operational and strategic objectives.

7. **Documentation and Reporting:**
   Findings were documented in a structured format that supports executive understanding, highlights areas of risk or opportunity, and emphasizes the agency's progress toward robust access management practices.

5. Conclusion

Asset Lifecycle Management Controls

Purpose: The purpose of this audit is to provide assurance that AASHTOware applications are effectively governed and that access controls are designed to protect critical operational information, support operational continuity, and align with organizational objectives. Strong access management ensures that users and systems are appropriately identified, authenticated, and authorized, reducing the risk of unauthorized access while maintaining traceability and accountability. A robust access management program helps the agency comply with mandatory DIS-200 security requirements, safeguard information assets, and support strategic decision-making by providing confidence in system integrity and operational reliability. This audit focused on the extent to which AASHTOware access management practices support these outcomes.

Inherent Risk: The audit leveraged the control framework established in the Department of Administration's prior DIS-200 audit as a foundation for evaluating risk. We considered the inherent risk associated with unauthorized access, inappropriate privilege allocation, insufficient authentication, session misuse, and incomplete monitoring or auditability. This risk-informed perspective allowed us to focus on the areas of greatest potential impact to agency operations, data security, and regulatory compliance. The audit evaluated processes providing insight into organizational practices, governance, and strategic alignment.

This engagement demonstrates the agency's commitment to strong access governance for the AASHTOware systems. By focusing on process effectiveness and principle-based controls, the audit provides assurance that management has established a structured approach to protect information assets, enforce accountability, and align access practices with operational and strategic priorities. The review highlights the agency's foundation for ongoing improvement, supporting the secure, efficient, and resilient use of AASHTOware applications across its operations.

Observations and Recommendations

We collaborated with Engineering, Finance and Administration, and Information Technology to develop the observations and recommendations for remediating any discovered deficiency. IAS and SCDOT Executive Leaders discussed these observations and recommendations.

Development of Management Action Plans

We facilitated Management's development of action plans for each observation and/or performance opportunity to improve control design with practical, cost-effective solutions. These improvements, if effectively implemented, are expected to reduce the overall risk exposure to an acceptable level (i.e. within the Agency's risk appetite).

We will follow up with Management on the implementation of the proposed actions on an ongoing basis and provide SCDOT leadership with periodic reports on the status of management action plans and whether those actions are effectively and timely implemented to reduce risk exposure to an acceptable level.

Reporting of Confidential Information

Due to the confidential nature of information security, the observations, recommendations, and management action plans are not included in this report. This information is not considered or deemed "public record" in accordance with the SC Freedom of Information Act pursuant to SC Code of Laws Section 30-4-20 (c) which states that information relating to security plans and devices proposed, adopted, installed, or utilized by a public body, other than amounts expended for adoption, implementation, or installation of these plans and devices, is required to be closed to the public and is not considered to be made open to the public under the provisions of this act.

Appendix A - Process Descriptions

Process Overview

The effective management of application security and access management within the AASHTOware suite is a critical enabler of operational efficiency, security, and regulatory compliance. While adherence to mandatory DIS-200 requirements establishes a baseline of security, a strategic, lifecycle-based approach allows the agency to move beyond compliance toward a more mature, risk-informed posture. By embracing structured governance, proactive planning, continuous monitoring, and timely adjustments, the agency can reduce exposure to unauthorized access, strengthen accountability, and enhance confidence in system integrity. This lifecycle perspective aligns with the intent of DIS-200 standard, where access management processes are consistently applied, documented, and optimized to support both business objectives and a dynamic risk environment.

Application Security & Access Management Process Overview

Governance & Policy: Establish executive oversight, clarify roles and responsibilities, and define high-level expectations for access management and user/account accountability.

Planning & Design: Identify the types of accounts, roles, and access levels required to support business objectives, operational needs, and regulatory requirements.

Provisioning & Onboarding: Assign accounts and roles according to defined policies, ensuring that access aligns with job responsibilities and segregation-of-duties considerations.

Monitoring & Adjustment: Continuously monitor access activity, review account privileges, and adjust roles as operational needs or risks change.

De-provisioning & Offboarding: Remove or modify access promptly when accounts are no longer needed, roles change, or staff transition out of responsibilities.

Oversight & Continuous Improvement: Evaluate the effectiveness of access management processes, incorporate lessons learned, and adapt policies and practices to maintain alignment with agency goals, compliance requirements, and evolving risks.

Appendix B – Generic Maturity Model

Maturity Level		Description
1	**Initial**	• Roles and responsibilities are not formally defined. • Processes are ad hoc, undocumented, and vary across teams. • **Success depends on individual efforts, not repeatable** *Governance is informal or absent*.
2	**Managed**	• **Some policies and procedures are documented and implemented, but coverage is inconsistent across teams/ divisions/ organization**. • Processes are repeatable in limited areas and lack organization-wide coordination. • Processes typically reflect baseline requirements or team-level priorities but lack organization-wide governance. *Governance is reactive and localized*.
3	**Defined**	• Policies, procedures, and standards are documented and • **Processes are designed to ensure consistency and** • Gaps and risks in the process begin to be recognized beyond *Governance is structured and organization-wide*.
4	**Quantitatively Managed**	• Processes are consistently implemented and measured across the organization. • **Performance measures are used to evaluate process effectiveness, identify risks, and drive decisions**. • Risk-based process adjustments are regularly made to improve outcomes. *Governance is proactive and data-informed**.
5	**Optimizing**	• **A culture of continuous improvement is embedded** • Feedback loops, innovation practices, and lessons learned are • Metrics and improvement goals are routinely reviewed and *Governance is strategic and embedding in the culture*.

Data-informed – Using data as a key input to guide decisions, while also considering human judgement, experience, and strategic priorities.